



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
SISTEMA DE POSGRADO
MAESTRÍA EN DERECHO CONSTITUCIONAL**

TEMA:

El acceso a las Tecnologías de la Información y Comunicación (TICS) como derecho establecido en la constitución del Ecuador de 2008 y su efecto sistemático de vulneración de derechos de los ciudadanos.

AUTOR:

**Abg. Omar Gerard Altamirano Villena.
MAGISTER EN DERECHO CONSTITUCIONAL
Trabajo de Titulación proyecto de investigación para la Obtención del Grado de
Magister en Derecho Constitucional**

TUTOR:

ABG. KLEBER DAVID SIGUENCIA SUAREZ, Mgtr.

Guayaquil, Ecuador

11 de noviembre del 2021



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**

SISTEMA DE POSGRADO

MAESTRÍA EN DERECHO CONSTITUCIONAL

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el abogado, Omar Gerard Altamirano Villena, como requerimiento parcial para la obtención del Grado Académico de Magister en Derecho Constitucional.

**Abg. Kleber David Siguencia Suarez, Mgtr.
DIRECTOR DE PROYECTO DE INVESTIGACIÓN**

**REVISORA
Lcda. María Verónica Peña Seminario, Ph. D
Nuria Pérez Puig-Mir Ph. D**

**Abg. Miguel Hernández Terán, Phd.
DIRECTOR DEL PROGRAMA**

Guayaquil, a los 11 días del mes de noviembre del año 2021



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
SISTEMA DE POSGRADO**

MAESTRÍA EN DERECHO CONSTITUCIONAL

DECLARACIÓN DE RESPONSABILIDAD

Yo, Altamirano Villena Omar Gerard

DECLARO QUE:

El Proyecto de Investigación **El acceso a las Tecnologías de la Información y Comunicación (TICS) como derecho establecido en la constitución del Ecuador de 2008 y su efecto sistemático de vulneración de derechos de los ciudadanos**, previa a la obtención del **Grado Académico de Magister en Derecho Constitucional**, ha sido desarrollada en base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de investigación del Grado Académico en mención.

Guayaquil, a los 11 días del mes de noviembre del año 2021

EL AUTOR

Abg. Omar Gerard Altamirano Villena



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
SISTEMA DE POSGRADO
MAESTRÍA EN DERECHO CONSTITUCIONAL**

AUTORIZACIÓN

Yo, autorizo a la Universidad Católica de Santiago de Guayaquil, la **publicación** en la biblioteca de la institución del **Proyecto de Investigación Magister en Derecho Constitucional** titulada: **El acceso a las Tecnologías de la Información y Comunicación (TICS) como derecho establecido en la constitución del Ecuador de 2008 y su efecto sistemático de vulneración de derechos de los ciudadanos**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 11 días del mes de noviembre del año 2021

EL AUTOR

Abg. Omar Gerard Altamirano Villena

REPORTE URKUND

URKUND Abrir sesión

Documento: TESIS AB OMAR ALTAMIRANO (REVISIÓN URKUND).doc (D:16240895)

Presentado: 2021-11-11 10:08 (-05:00)

Presentado por: viviana.betty@yahoo.com

Recibido: miguel.hernandez_ucsg@analysis.orkund.com

Mensaje: TESIS AB OMAR ALTAMIRANO (URKUND 2DA REVISION) [Mostrar el mensaje completo](#)

3% de estas 63 páginas, se componen de texto presente en 7 fuentes

Lista de fuentes Bloques

Categoría	Enlace/nombre de archivo
	TESIS FINAL COMPLETA SIN INDICE CARMEN [1].docx
	TESIS Susy Sacoto.docx
	Maria Gabriela Herrera Romero, La Aplicación y cumplimi...
	http://repositorio.sagratoro.edu.ec/bitstream/1234567
	https://www.ibm.com/developerworks/sa/local/im/que
	http://www.infodiv.mx/index.php?botones/solicita
	https://www.lifeder.com/investigacion-bibliografica/tr-1
	Fuentes alternativas
	Fuentes no usadas

0 Advertencias Reiniciar Compartir

“Los móviles son el sueño de Stalin, porque emiten cada dos o tres minutos una señal de ubicación. Y peor aún, uno de sus procesadores tiene una puerta trasera universal que los convierte en dispositivos de escucha que no se apaga nunca”.

RICHARD STALLMAN¹

“La computación en la nube constituye un peligro para la libertad en Internet”.

VINCENT MOSCO²

“Aquellos que renuncian a una libertad esencial para comprar un poco de seguridad momentánea, no merecen ninguna de las dos”.

BENJAMIN FRANKLIN³

"La inteligencia artificial augura el fin de la raza humana".

STEPHEN HAWKING⁴

¹ Richard Stallman: Nació en Nueva York 1953. Creador del software libre (Gnu 1984, Linux 1992), creador del concepto copyleft, que dio lugar a las creative commons.

² Vincent Mosco: Profesor emérito de Sociología en la Queen’s University de Kingston, Ontario (Canadá). Analista de las transformaciones en la comunicación y de los medios, además de ser promotor de la Canadian Social Sciences and Humanities Research Council.

³ Benjamin Franklin: Nació el 17 de enero de 1706, Milk Street, Boston, Massachusetts, Estados Unidos, murió el 17 de abril de 1790, Filadelfia, Pensilvania, Estados Unidos Fue un político, polímata, científico e inventor estadounidense. Es considerado uno de los Padres Fundadores de los Estados Unidos.

⁴ Stephen William Hawking: Nació el 8 de enero de 1942 en Oxford, Reino Unido y murió el 14 de marzo de 2018 en Cambridge, Reino Unido. Fue un físico teórico, astrofísico, cosmólogo y divulgador científico británico.

AGRADECIMIENTO

Quiero agradecer a todas las personas que me han ayudado para finalizar el presente trabajo, tanto a los conocidos y amigos que se han tomado su tiempo para responder y compartir las encuestas enviadas por las plataformas de redes sociales, de la misma manera a los compañeros y amigos Jueces e Ingenieros en Sistemas del Departamento de TICs de la Corte Provincial del Guayas respectivamente, los mismos que han sido tan generosos con su tiempo brindado para responder a mi entrevista planteada, compartiendo sus conocimientos y experiencias.

Abg. Omar Gerard Altamirano Villena

DEDICATORIA

Dedico la presente Tesis a Dios y a mi madre; guías en la dirección que debo de transitar para crecer cómo ser humano y a nivel profesional, con el fin de aportar mis conocimientos a la sociedad, con el anhelo de contribuir para bien en un mundo caotizado por ideologías y dogmas que desvirtúan la esencia del ser humano, al mismo tiempo que se aleja de su esencia divina, generando el caos. Por lo cual, es menester contribuir activamente para regular las anomalías generadas, con el fin de lograr hacer un mejor mundo, tanto físico como digital, en el cual podamos vivir e interactuar en armonía.

Abg. Omar Gerard Altamirano Villena

ÍNDICE

CERTIFICACIÓN	II
DECLARACIÓN DE RESPONSABILIDAD.....	III
AUTORIZACIÓN	IV
PRINT URKUND.....	V
AGRADECIMIENTO	VII
DEDICATORIA	VIII
ÍNDICE.....	IX
RESUMEN	XVIII
ABSTRACT.....	XIX
INTRODUCCIÓN	2
CAPITULO I	3
PLANTEAMIENTO DE LA INVESTIGACIÓN (ANTECEDENTES)	3
1.1. Objeto de estudio.....	3
1.1.1. Problema General.....	3
1.1.2. Problema Específico.....	3
1.2. Campo de acción.....	3
1.3. Planteamiento del problema.....	4
1.3.1. Justificación	5
1.3.2. Preguntas de investigación.....	6
1.3.3. Objetivos de la investigación	7
1.3.4. Hipótesis	7
CAPITULO II.....	8
MARCO TEÓRICO.....	8

2.1. Antecedentes.....	8
2.2. Marco teórico conceptual.....	11
2.2.1. Sociedad de la información y del conocimiento.....	11
2.2.3. Nuevas tecnologías de la información y comunicación (NTICs).	13
2.2.4. Herramientas de las nuevas tecnologías de la información y comunicación (NTICs).....	15
2.2.5. Ventaja del uso de las TICs.	18
2.2.6. Desventaja del uso de las NTICs.	19
2.3. Marco referencial.....	22
2.3.1. Las tecnologías.....	22
2.3.2 TICs (Tecnologías de la Información y Comunicación).....	22
2.3.3. Redes Sociales	22
2.3.4. Big Data	23
2.3.5 Inteligencia Artificial.....	23
2.3.6. Tratamiento de datos.....	23
2.3.7 Internet	23
2.3.8. Videocámaras y video vigilancia	24
2.3.9. Teléfono inteligente o Smartphone	24
2.3.10. Cadena de bloques o Blockchain.	24
2.4 Marco legal.	25

2.4.1. Teoría constitucional.....	25
2.4.2. Legislación de la Unión Europea con respecto a la protección de datos personales.....	34
2.4.3. Instrumentos internacionales.	34
2.4.4. Sistema Interamericano de Protección de los Derechos Humanos (SIDH)...	36
2.4.5. Pronunciamiento legal en países Hispanoamericanos.	37
2.4.6. Normativas jurídicas que rige la protección de datos en el Ecuador.	38
2.4.7. Pronunciamiento de la Corte Constitucional del Ecuador.	41
CAPITULO III.....	45
MARCO METODOLÓGICO.....	45
3.1. Tipo y diseño de la investigación.	45
3.1.1. Diseño.....	45
3.2. Enfoque.....	46
3.2.1. Cualitativa	46
3.2.2. Cuantitativa	46
3.2.3. Descriptivo	47
3.3. Población y muestra.....	47
3.3.1. Características de la población.....	47
3.3.2. Delimitación de la población.....	47
3.3.3. Tipo de muestra.....	47
3.3.4. Tamaño de la Muestra	48

3.4.	Proceso de selección de la muestra.....	48
3.5.	Los métodos y las técnicas.	49
3.5.1.	Métodos Teóricos.....	49
3.5.2.	Método Analítico Sintético	49
3.5.3.	Método analítico.....	49
3.6.	Técnicas o instrumentos.	49
3.6.1.	Encuesta	49
3.6.2.	Entrevista a Expertos.....	50
3.7.	Criterios de inclusión.....	50
3.8.	Gestión de los datos.....	50
3.9.	Hipótesis del estudio.....	50
3.10.	Variables operativas, indicadores y parámetros aplicados.....	51
3.10.1.	Operacionalización de variables.....	51
CAPITULO IV.....		66
ANÁLISIS DE LOS RESULTADOS		66
4.1.	Conclusiones Parciales.	66
4.1.1.	Encuesta de uso de TIC.....	66
4.1.2.	Exposición y análisis de los resultados recabados mediante encuestas realizada a los ciudadanos del cantón Guayaquil.	68
4.1.3.	Análisis e interpretación de los datos recabados mediante entrevista realizada a expertos.....	81

4.1.4. Conclusiones.....	95
4.1.5 Discusión.....	99
4.1.6 Comprobación de hipótesis.....	102
CAPITULO V.....	102
LA PROPUESTA DE INTERVENCIÓN	102
5.1. Introducción.....	102
5.2. Objetivo.....	104
5.3. Factibilidad	104
5.4. Descripción	105
5.5. Resultados Esperados.....	110
CAPITULO VI.....	111
CONCLUSIONES Y RECOMENDACIONES	111
6.1. Conclusiones	111
6.2. Recomendaciones	114
6.3. Limitaciones.....	116
CAPITULO VII	117
REFERENCIAS BIBLIOGRÁFICAS.....	117
VIII.....	125
APÉNDICE.....	125

ÍNDICE DE TABLAS

Tabla 1. Normativas jurídicas que rige la protección de datos en el Ecuador.	41
Tabla 2. Población	47
Tabla 3 Delimitación de la población.	47
Tabla 4. Definición conceptual de variables.	51
Tabla 5. Operacionalización de variables – Encuestas.	60
Tabla 6. Operacionalización de variables – Entrevistas.	65

ÍNDICE DE GRÁFICOS

Gráfico 1. Rango de uso de TICs a nivel nacional.	66
Gráfico 2. Uso de TICs en el cantón Guayaquil Prov. del Guayas.	67
Gráfico 3. Características etarias.	68
Gráfico 4. Sexo.	69
Gráfico 5. Instrucción Educativa.	69
Gráfico 6. Opinión sobre acceso a TIC y vulneración de derechos.	70
Gráfico 7. Derechos que se ven perjudicados por acceso a TICs.	71
Gráfico 8. Medio por el que TIC puede vulnerar sus derechos.	71
Gráfico 9. Opinión sobre uso de Redes sociales y vulneración de derechos.	72
Gráfico 10. Redes sociales por las que puede vulnerar sus derechos.	73
Gráfico 11. ¿El Sistema de cámaras de vigilancia de ECU911 puede vulnerar sus derechos?.....	73
Gráfico 12. ¿Derechos que se vulneran por uso de Sistemas de vigilancia ECU 911?	74
Gráfico 13. ¿Las empresas del Estado puede vulnerar sus derechos?	75
Gráfico 14. ¿Redes sociales por las que puede vulnerar sus derechos?.....	75
Gráfico 15. ¿Empresas que venden la información pueden vulnerar sus derechos?	76
Gráfico 16. ¿Derechos que pueden vulnerar empresas que venden la información?	77
Gráfico 17. ¿Derechos a decidir sobre el uso de su información personal?	77
Gráfico 18. ¿Debe haber un derecho para eliminar la información generada o compartida?	78
Gráfico 19. Respuesta de las Instituciones públicas frente al ciberdelito.....	79

Gráfico 20. Opinión ciudadana sobre la tarea legislativa en el área de tecnología y tratamiento de datos personales.	80
Gráfico 21. Red de resultado de la encuesta aplicada.....	95
Gráfico 22. Nube de palabras generada de las entrevistas a expertos.	98

ÍNDICE DE ANEXOS

Anexo 1. Encuesta de opinión para la ciudadanía	125
Anexo 2. Resultados de la encuesta de opinión ciudadana.....	133
Anexo 3. Entrevista a expertos sectoriales.	141
Anexo 4. Resultados individuales de la entrevista desarrollada a expertos sectoriales..	144

RESUMEN

A partir de que la Organización de las Naciones Unidas (ONU) declaró el acceso a internet como un derecho humano, instando a los gobiernos a facilitar su acceso, mencionando que es una herramienta que facilita el crecimiento y progreso de las sociedades, además de la utilidad para ejercer el derecho a la libertad de expresión, muchos países incluyendo a Ecuador han creado profundas reformas en sus leyes para lograr este objetivo, es así que la Constitución de la República del Ecuador del 2008, establece el derecho al acceso de las Tecnologías de la Información y Comunicación de los ciudadanos ecuatorianos, con el fin de integrar a los ciudadanos a la sociedad de la información y del conocimiento, asegurando el acceso y uso del internet.

Sin embargo, en la práctica existen perjuicios que atentan tanto al ciudadano individual, como a la sociedad. Al ejercer el derecho al acceso de las TICs, la falta de conocimiento y capacitación de su debida aplicación, sumada la irresponsabilidad del ciudadano, además de una deficiente legislación en la materia, se generan violaciones a los derechos de los ciudadanos; violaciones realizadas no sólo por las empresas tecnológicas con su recolección y tratamiento de datos, sino también por los gobiernos de los Estados al ejercer políticas públicas de control.

En la actualidad, la irrupción de la tecnología es abrumadora, su desarrollo acelerado, es una debilidad del derecho que evoluciona de forma lenta y paulatina, por lo cual, valiéndose de la democratización del acceso a las TICs, en la cual los usuarios crecen, los datos han reemplazado al petróleo, siendo su utilización y aplicación para fines comerciales y políticos no ha conocido limites, causando perjuicios y por ende violaciones de derechos, los cuales se han expuesto en el presente estudio.

Palabras claves: Vulneración de Derechos, Derecho a la privacidad, Internet, Ciudadanos, Gobierno, Empresas tecnológicas, TIC, Tecnología, Redes Sociales, aplicaciones, cámaras de vigilancia, Datos, Tratamiento de Datos personales.

ABSTRACT

Since the United Nations Organization declared access to the internet as a human right, urging governments to facilitate its access, mentioning that it is a tool that facilitates the growth and progress of societies, as well as the utility to exercise the right to freedom of expression, many countries including Ecuador have created profound reforms in their laws to achieve this objective, thus the Constitution of the Republic of Ecuador of 2008 establishes the right of access to Information and Communication Technologies of Ecuadorian citizens, in order to integrate citizens to the information and knowledge society, ensuring access and use of the internet.

However, in practice there are damages that affect both the individual citizen and society as a whole. By exercising the right to access ICTs, the lack of knowledge and training in its proper application, added to the irresponsibility of the citizen, in addition to a deficient legislation on the matter, violations of citizens' rights are generated; violations carried out not only by technology companies with their data collection and processing, but also by state governments when exercising public control policies.

At present, the irruption of technology is overwhelming, its accelerated development, is a weakness of the law that evolves slowly and gradually, therefore, using the democratization of access to ICTs, in which users grow, the data have replaced oil, being its use and application for commercial and political purposes it has not known limits, causing damages and therefore violations of rights, which have been exposed in this study.

Keywords: Violation of Rights, right to privacy, Internet, Citizens, Government, Technology companies, ICT, Technology, Social Networks, applications, surveillance cameras, Data, Personal Data Processing.

INTRODUCCIÓN

El conocimiento abierto se define como conocimiento accesible, libre de uso, y gratuito a su usuario. Este concepto es parte de un movimiento que busca generar soluciones para el bien público de manera colaborativa. La protección de datos personales viene teniendo una fuerte discusión, desde mucho antes que pasara el incidente de los wikileaks, la comunidad internauta es una de las principalmente afectadas, aunque en la práctica, más personas naturales y jurídicas se suman a las protestas por la revolución tecnológica que ha provocado liberación de códigos en plataformas tecnológicas que captan información desde diversos métodos.

El 25 de mayo de 2018, el Reglamento General de Protección de Datos (“GDPR”) de la Unión Europea (UE) entró en vigor, provocando que varios países latinoamericanos reformaran y actualizaran su legislación local sobre protección de datos personales. Brasil, Chile, Argentina y México han tomado medidas para aumentar la protección de la privacidad y la seguridad de los datos personales de sus ciudadanos. En 2019, la protección de datos personales estuvo en portadas en todo el mundo: India se encontró debatiendo su primera ley de protección de datos, el abuso de datos personales fue un tema central de las elecciones en Túnez, la Unión Europea celebró el primer aniversario de su Reglamento General de Protección de Datos (GDPR), y mucho más.

Las grandes bases de datos (big data), son un compendio de las maravillas de millones de datos que corren por los canales de internet desde las redes sociales, la aplicación de códigos para segmentar el mercado según sus propios intereses es una práctica que cada día se hace más recurrente. Cuanto más se recopilan, retienen y explotan los datos de forma rutinaria, ya sea por el sector público o privado, más urgente es implementar leyes y políticas públicas de protección de datos. Nuestra información se encuentra cada vez más en riesgo, ya sea que se trate de la historia clínica, los chats en redes sociales, las compras en línea, la información sobre nuestra ubicación o cualquier otra información que pueda ser recolectada y usada para manipular o controlarlos. Por ello los gobiernos y las empresas deben actuar ahora para protegerla. Los individuos más vulnerables de la sociedad como los activistas, periodistas, defensores de derechos humanos y miembros de grupos marginalizados u oprimidos son los que se encuentran más expuestos a esta amenaza.

CAPITULO I

PLANTEAMIENTO DE LA INVESTIGACIÓN (ANTECEDENTES)

1.1. Objeto de estudio.

1.1.1. *Problema General*

Deficiencia en la regulación y control del Estado en lo que corresponde al tratamiento de datos de los ciudadanos al ejercer el derecho constitucional del acceso a las Tecnologías de la Información y Comunicación (TICs), por cuanto, es un derecho que genera derechos, así mismo podría vulnerar derechos, desde su desarrollo, hasta la utilización de los mismos, es así, que los ciudadanos corren el riesgo de ser víctimas, pudiendo verse lesionados o vulnerados sus derechos, tanto fundamentales como humanos.

1.1.2. *Problema Específico*

Deficiente normativa, en cuanto a regulaciones legales en lo que respecta al tratamiento de datos personales en el Ecuador; en cuyas normativas se debería establecer el control al propio Estado y a Empresas o Multinacionales.

Proceso de vigilancia de los ciudadanos, con el cual se provoca violaciones de derechos, como: Derecho a la privacidad e intimidad, libertad de expresión, huelga, libertad de tránsito, etc.

Peligro progresivo al limitar el derecho a la libertad y libre movilidad de tránsito, por el control ejercido a los ciudadanos, mediante aplicaciones tecnológicas de geolocalización, vigilancia, así como de reconocimiento facial.

Dictadura de los medios de comunicación y plataformas tecnológicas: limitación a la libertad de expresión y de pensamiento, por ausencia de regulaciones legales.

1.2. Campo de acción.

Campo: Jurídico.

Área: Derecho Constitucional y Derechos Humanos.

Tema: El acceso a las tecnologías de la información y comunicación (TICs) como derecho establecido en la constitución del Ecuador de 2008 y su efecto sistemático de vulneración de derechos de los ciudadanos.

Delimitación Espacial: La presente investigación está enfocada a desarrollarse en conjunto con los ciudadanos, entre ellos, especialistas en áreas de la tecnología, así como abogados expertos en derechos humanos y derecho constitucional.

El presente estudio se centra entre las áreas del conocimiento jurídico de los Derechos Humanos y el Derecho Constitucional, frente al uso de las nuevas tecnologías, con su entorno digital y sus efectos en el mundo físico.

1.3. Planteamiento del problema.

El acceso a las Tecnologías de la Información y Comunicación (TIC) es reconocido en la Constitución de la República del Ecuador de 2008 como un derecho, el cual permite a los ciudadanos acceder sin restricciones al uso de las TIC y por ende a plataformas tecnológicas como páginas web o redes sociales, para así facilitar la democratización de la información en la era del conocimiento, así mismo para generar las condiciones que permitan que la comunicación sea más efectiva y global.

Si bien es cierto, la irrupción de las tecnologías en la habitualidad de la sociedad ha generado un cambio exponencial, el mismo que ha sido acogido por los ciudadanos – aprendiendo rudimentariamente a utilizar los dispositivos tecnológicos, los mismos que por encontrarnos en un país relativamente democrático y capitalista, se puede acceder a ellos, en variedad de precio y sin limitaciones o restricciones-, pero ese proceso ha sido sin capacitación previa, mucho menos asumiendo responsabilidades por parte de los ciudadanos, sin ninguna diferencia en comparación con la generación de los nativos tecnológicos.

El papel de la Función Legislativa del Estado no ha reaccionado ágilmente en la era tecnológica, adaptando, reformando y generando leyes que controle a las empresas tecnológicas, así mismo limite a los gobiernos, con el fin de proteger los derechos de los ciudadanos que en el proceso de su aceptación, adaptación y uso tecnológica, pueda causar vulneraciones de derechos, por cuanto así como éste derecho de acceso a las TIC es generador derechos, también tiene efectos contraproducentes, por cuanto, el uso de tecnología implica la producción de datos personales, los mismos que en esta nueva era se han convertido en fuente de ganancias, estando el ser humano a merced de las empresas tecnológicas y los gobiernos, cuando debería ser todo lo contrario.

1.3.1. Justificación

La presente investigación expone fundamentos teóricos acerca de las TICs y plataformas tecnológicas que trabajan en sinergia, así como su marco legal vigente en Ecuador, que permite iniciar la discusión sobre la legalidad y posible vulneración de derechos humanos y fundamentales que podrían sufrir los ciudadanos al encontrarse en un entorno tecnológico o los usuarios de internet y de plataformas de información y comunicación, que forman parte de las TICs.

La tecnología se ha desarrollado vertiginosamente en los dos últimos siglos, siendo impulsada y desarrollada por empresarios y figuras políticas de gobiernos de turno del primer mundo, para ser utilizada, ya sea en defensa de la soberanía nacional, control y seguridad interna, por lo que su aporte teórico es fundamental para entender en qué medida se podría afectar los derechos de los usuarios y/o consumidores de la tecnología.

En cuanto a la aportación metodológica es importante destacar conforme a la opinión de los usuarios y/o consumidores, la percepción sobre el objeto de estudio, esta metodología aplicada se interna no solo en la visión de los consumidores, sino en la visión de los abogados y personal del Consejo de la Judicatura, quienes usan un sistema informático de alto nivel, con un soporte técnico del departamento de TICs, con quienes desarrollan experiencia diariamente al utilizar las tecnologías de la información y comunicación al administrar justicia, siendo propicio para entender de fuente primaria, cuáles son los principales mecanismos utilizados para sustanciar procesos hasta llegar a dictar sentencia que podrían acarrear sanciones, conforme el marco legal ecuatoriano.

El aporte pragmático de la presente investigación se centra en que el desarrollo tecnológico abre un abanico de posibilidades, es así que, la tecnología no solo es aplicada para la vigilancia de ciudades, ocasionando vulneración de derechos como el derecho a la intimidad de los ciudadanos, además del derecho a la movilidad personal, también para guiar la opinión pública de la ciudadanía, a través de las redes sociales, incidiendo en el derecho de la libre elección en un régimen democrático.

Particularmente en el caso de Ecuador, contribuye a demostrar qué en todo el país hay más de cuatro mil cámaras de vigilancia que receptan y envían capturas de video a centros de monitoreo donde las grabaciones son examinadas por servidores públicos, cómo funcionarios,

policías y el servicio de inteligencia, actos que propician la vulneración de derechos, por cuanto el consentimiento de la ciudadanía ha pasado por alto.

En cuanto al ámbito social desde el punto de vista de derechos de los ciudadanos, los consumidores de las grandes telefónicas y empresas ecuatorianas, no cuentan con información sobre las acciones que pueden llevar a cabo por el uso de sus datos, los mismos que obtienen sin consentimiento, generando una autorización forzada o desconocida por el ciudadano para su tratamiento; obteniendo información de índole personal, como crediticia, siendo recopiladas por la gestión de las empresas para luego vender los archivos o base datos a empresas que lo requieran, conociendo que pueden ser utilizadas en el ámbito comercialmente, pero podría darse el riesgo que con la información puedan cometer delitos.

Finalmente, el presente estudio se hace viable debido a que los sujetos de estudio y los aspectos metodológicos son accesibles al investigador, por lo que la información es accesible y disponible. Por tanto, es imprescindible realizar el presente estudio, para determinar si los ciudadanos al ejercer el derecho al acceso de las TICs, se han visto, se ven o se verán vulnerados, con el fin de llegar a establecer recomendaciones para evitar se cometan abusos y violaciones a vuestros derechos, propiciando la propuesta de implementar un marco legal que exija a las empresas tecnológicas, empresas de consultoría que utilicen datos, así como a los gobiernos de turno que respeten nuestros derechos humanos y fundamentales.

1.3.2. Preguntas de investigación

¿Qué tipo o elementos de Tecnologías de la Información y Comunicación (TIC), son más accesibles para el uso por parte de los ciudadanos?

¿Cuáles son los efectos contraproducentes generados por las empresas o los intermediarios que manejan plataformas tecnológicas?

¿Qué tipos de elementos tecnológicos instalan los gobiernos de los Estado para la seguridad y control nacional?

¿Cuál es el motivo que insta a los gobiernos a invertir en tecnología de control ciudadano?

¿Cuáles son los efectos que probablemente puede generar la automatización tecnológica del Estado con respecto a los derechos de los ciudadanos?

¿Por qué se reconoce el acceso a las TIC como un derecho en la Constitución del Ecuador?

¿Cuáles son los mecanismos de protección legal del tratamiento de datos personales en el Ecuador?

¿Cómo es el proceso de protección de los derechos con respecto a los datos personales en el Ecuador?

¿La Corte Constitucional del Ecuador ha tomado alguna postura en lo que respecta a la protección de datos personales, para salvaguardar los derechos de los ciudadanos?

1.3.3. Objetivos de la investigación

1.3.3.1. Objetivo General.

Analizar la actuación del Estado ecuatoriano en lo que respecta a la vulneración de derechos provocados por el uso indiscriminado de los datos, obtenidos a través de las TIC en el país.

1.3.3.2. Objetivo Específicos

- Identificar el entorno legal y operativo en el que se utilizan las TIC dentro de la sociedad ecuatoriana.
- Investigar los pronunciamientos de la Corte Constitucional del Ecuador sobre vulneración de derechos en el ámbito tecnológico.
- Desarrollar una propuesta de intervención que garantice el respeto a la privacidad de las personas, en un entorno justo y equitativo.

1.3.4. Hipótesis

1.3.4.1. Hipótesis General.

El uso de las TICs y plataformas tecnológicas como páginas web y redes sociales, vulneran los derechos de los ciudadanos ecuatorianos, por la deficiente legislación que regule el tratamiento de datos.

1.3.4.2. Hipótesis Específica.

Las TICs más utilizadas por los ciudadanos y el Estado son: la televisión, la radio, el internet, el teléfono inteligente y computadoras.

Los gobiernos al instalar y utilizar masivamente cámaras de seguridad computarizadas vulneran derechos de los ciudadanos como el derecho a la libre movilidad de tránsito y derecho a la protesta.

Las empresas de plataformas tecnológicas al obtener, almacenar y procesar datos personales, vulneran el derecho a la privacidad de datos personales.

Las plataformas tecnológicas, como páginas web y redes sociales, con el procesamiento de datos y su deficiente control de reserva de datos, vulneran el derecho a la privacidad, el derecho a la imagen y buen nombre de las personas.

Los efectos de la automatización del Estado es el control y la limitación de derechos del ciudadano como, el derecho a la libre movilidad y el derecho a la privacidad personal.

En Ecuador la Asamblea Nacional en el presente año dos mil veintiuno expidió la Ley de Protección de Datos Personales agregándola a la legislación interna, no siendo de inmediata aplicación las medidas correctivas y el régimen sancionatorio por un periodo de tiempo, contando con la garantía jurisdiccional de Habeas Data, la que se encuentra muy limitada a los avances tecnológicos, creando incertidumbre jurídica en ésta área.

La legislación vigente ecuatoriana contempla la Garantía Jurisdiccional como el Habeas Data, como mecanismos legales en el área de datos personales, encontrándose en espera la aplicación progresiva de la Ley de Protección de Datos Personales y la creación de jurisprudencia.

CAPITULO II

MARCO TEÓRICO

2.1. Antecedentes.

El interés por el análisis del acceso a las TICs, como derecho establecido en la constitución del Ecuador del 2008, nace por la interrogante planteada, en la cual la tecnología se ha desarrollado de manera exponencial en sus diversas innovaciones, ya que ha sido impulsada

por inversiones para el desarrollo de tecnología militar para ser aplicadas en la protección de la soberanía de países o en conflictos bélicos, apoyado por el capitalismo en gobiernos democráticos, así mismo siendo impulsado en gobiernos autoritarios o totalitarios, entrando en los últimos años China en la carrera tecnológica y armamentista con su modelo político híbrido, pasó hacer la fábrica del mundo, aprovechándose de la tecnología aportada y transmitida por países que necesitaban su mano de obra barata para fabricar sus diversos equipos, es así que el gigante de oriente copió, adaptó y desarrolló su propia tecnología y se encuentra en constante evolución.

Es así que la tecnología en las últimas décadas cómo primera instancia a estado desarrollada e implementada para los círculos de poder, así como para los gobiernos, sin distinción de ideologías políticas, tan sólo para ejercer y mantener el poder, es así que Almada Torres, (2020) menciona que:

El Ministerio para la Seguridad del Estado de la República Democrática de Alemania. También conocido por sus iniciales STASI, es conocido como una policía secreta que consiguió establecer una red que intervenía teléfonos no solo a nivel nacional, por lo que se infiltraba en movimientos políticos y reportaba relaciones personales y familiares de los ciudadanos del país comunista.

En opinión al autor Almada Torres (2020), manifiesta que “el patrón de vigilancia y control civil que establece la STASI ha sido desde aquel entonces un modelo a seguir para los regímenes autoritarios que utilizan la represión para controlar a su ciudadanía. Sin embargo, al culminar la Guerra Fría y con la ola de democratización y el aparente éxito de la democracia liberal, estas habilidades policiales ya no eran factibles.”

En segunda instancia, el sistema capitalista ha hecho que los ciudadanos puedan acceder a un costo menor a las tecnologías, así se han empoderado efímeramente los ciudadanos por haberse permitido un mayor acceso a la información, generada por la economía que ha permitido su adquisición y por ende, al haber ese consumo masivo, ha experimentado un auge la democracia por la democratización de la información y la interacción de la sociedad civil.

Si bien es cierto la tecnología, siendo optimistas puede ofrecernos un futuro libre y democrático, con respeto a los derechos humanos, así como todo lo contrario, esto depende del

tipo de gobierno según su ideología se instale en el poder de los países en base al apoyo ciudadano, ya sean estos democráticos o totalitarios, tomando en consideración el auge del socialismo a nivel mundial, por sus tentadoras propuestas de un estado de bienestar; pero la realidad es que la libertad y respeto a los derechos humanos se encuentran en constante peligro, ya que los gobiernos totalitarios en mayor medida aprovechan la tecnología y utilizan métodos sofisticados, desarrollados para mantenerse en el poder.

En la investigación y entrevista desarrollada por France 24 Español (2019), en lo que respecta a China, determina que:

Existe una vigilancia permanente de sus ciudadanos, capaces de establecer su identidad en tiempo real, hasta el año 2019 mediante la tecnología se llegó a calificar sobre un puntaje de 950 el manejo de cuentas mediante un sistema, el que le obliga a portarse bien, siendo resultado el proceso por la recolección de datos, que catalogó cómo buenos y malos ciudadanos, utilizando el Big Data, mediante el cual todo será estudiado, como; la situación financiera, hábitos de consumo, la carrera profesional, incluso el comportamiento en las redes sociales. Criticar al gobierno en internet o exigir signos exteriores de riqueza conllevará a una mala calificación, por otra parte, elogiar al partido o donar sangre aumenta el crédito social. Un buen puntaje otorga ventajas, un mal puntaje quita derechos.

La Corte Suprema de china estableció la lista negra para los que tienen un mal puntaje de malos ciudadanos con nota cero. El reportaje desarrollado en Chonging, China, menciona que un periodista Liu Hu, se interesó demasiado en un caso de corrupción relacionado con un alto cargo del partido, fue condenado por un tribunal por difamación, por ello que según él, su nombre fue registrado en la lista negra de la noche a la mañana, dándose cuenta al comprar un ticket para el tren y que no lo dejarían viajar, juzgándolo como indigno de confianza, es así que una vez estando en la lista negra, no puede obtener un crédito bancario o crear un empresas, comprar un departamento o incluso inscribir a sus hijos en una escuela privada.

A este sistema lo catalogan cómo dictadura digital. El ciudadano chino Liu Hu, manifiesta que le preocupa porque considera que mucha gente perderá sus libertades individuales y que todos vivirán con restricciones.

Es así que es importante determinar al cuestionarse si el acceso a las TICs por parte de los ciudadanos, al haberse reconocido como un derecho fue el fin de asegurar su acceso, auto obligándose el estado a satisfacerlo, o podría ser el caso de facilitarse así el trabajo para que el estado y los gobiernos tenga el control de sus ciudadanos o para que algún autócrata que desee concentrar el poder, pueda hacerlo, llegando a utilizar la vigilancia permanente impulsada por algoritmos e inteligencia artificial y en el proceso pudiendo violentar derechos humanos. Trabajo que probablemente ha sido facilitado por la ONU⁵, ya que reconoció el acceso a internet como un derecho humano instando a los Estados a acatarlo.

Los gobiernos con el avance de la tecnología y aplicación de dispositivos banóptico aumentan la capacidad de los estados para controlar a las personas, en palabras de “Bigo propone el banóptico para indicar cómo las tecnologías de elaboración de perfiles se utilizan para determinar quién debe ser objeto de una vigilancia estricta” (Bauman & Lyon, 2013)

Es de vital importancia tratar de responder como garantizar las libertades esenciales y derechos, en países dirigidos por dictadores conforme menciona Bauman & Lyon (2013), “cuando el gobierno y la administración son dominadas por una sola persona o un partido, y éste utiliza el aparato administrativo con su archivos y datos como medio de control total” (p. 19).

Es así que las TICs son utilizadas como armas de control social, ayudados con sistemas de geolocalización, utilizándolo para rastrear a los ciudadanos, desarrollando así una vigilancia masiva imponiendo un Estado policial, los mismos que fácilmente pueden diseñar políticas públicas que sus efectos sean las restricciones de derechos, como el derecho a la libre expresión, derecho a la libertad de pensamiento, derecho de libre movilidad y el derecho a la intimidad, entre otros.

2.2. Marco teórico conceptual

2.2.1. Sociedad de la información y del conocimiento

La sociedad de la información es la que sufrió cambios y evoluciones, llegando al encuentro entre la sociedad civil, gobierno, organizaciones y facultades, utilizando mediante las TICs como herramienta que facilita notablemente la creación, la distribución, así como el uso de la información, siendo este factor indispensable para su desarrollo.

⁵ Organización de Naciones Unidas: Se fundó el 24 de octubre de 1945, mantiene su sede en la ciudad de Nueva York (Estados Unidos de Norte América).

Autores como Salvat y Serrano (2011), establecen que la Sociedad en la que la información pasa a convertirse en el factor decisivo de la organización económica, como consecuencia de la nueva tecnología digital, y que genera con ello cambios profundos en todos los ámbitos de la vida: culturales, políticos y sociales, sobre todo determinados por la transformación de las condiciones espacio-temporales de las interacciones entre los miembros de esa sociedad

La definición más acertada es la que nos proporciona en su página web el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (2021), determinando que:

La sociedad de la información es aquella que en las tecnologías que facilitan la instauración, distribución y manipulación de la información, estos juegan un papel importante en las actividades sindicales, culturales y económicas que debe estar centrada en la persona, integrada y orientada al desarrollo social, en que todos puedan crear, examinar, manejar y compartir la información y el discernimiento, para que las personas, las comunidades y las poblaciones puedan emplear plenamente sus posibilidades en el progreso de su desarrollo sostenible y en el avance de su calidad de vida.

Es importante destacar la definición de la sociedad de la información, proporcionada por Fernández Delpech el cual manifiesta que es “sucesora de la sociedad industrial, se refiere a la creciente capacidad tecnológica para almacenar informaciones y hacerlas circular cada vez de forma más rápida y con mayor difusión” (2016).

Por otra parte, la (OEA, 2009) manifiesta que la sociedad del conocimiento se refiere al tipo de sociedad que se necesita para competir y tener éxito frente a los cambios económicos y políticos del mundo moderno. Asimismo, se refiere a la sociedad que está bien educada, y que se basa en el conocimiento de sus ciudadanos para impulsar la innovación, el espíritu empresarial y el dinamismo de su economía.

Con lo manifestado se puede determinar que la sociedad del conocimiento precede a la sociedad de la información, por cuanto se pasó de generar información ya sea con fines comerciales o para tomar decisiones, a crear conocimiento y difundir los datos, en la que las

TICs y redes sociales juegan un rol determinante por aquellas relaciones sociales, culturales y hasta económicas, siendo efectiva para desarrollar una comunicación instantánea.

El conocimiento es el que propugna el desarrollo económico, propiciando los elementos para que se desarrolle la cuarta revolución industrial:

La cuarta revolución industrial, no obstante, no solo consiste en máquinas y sistemas inteligentes y conectados. Su alcance es más amplio. Al mismo tiempo, se producen oleadas de más avances en ámbitos que van desde la secuenciación genética hasta la nanotecnología, y de las energías renovables a la computación cuántica. Es la fusión de estas tecnologías y su interacción a través de los dominios físicos, digitales y biológicos lo que hace que la cuarta revolución industrial sea fundamentalmente diferente de las anteriores. (Schwab, 2016)

Si bien es cierto, la sociedad del conocimiento es un concepto ampliamente utilizado, es también cierto que las tecnologías que influyen como canales de comunicación merecen un espacio de mejora donde establecer políticas pensadas no solo en el uso de las plataformas como tal, sino en los contenidos que se manejan en las mismas. El entorno del conocimiento y de la información son intrínsecos, por tanto, no existiera conocimiento sin datos y viceversa. Sin embargo, es necesario que los elementos que influyen en su buen desempeño, se regulen a la necesidad de los consumidores.

2.2.3. Nuevas tecnologías de la información y comunicación (NTICs).

Menciona Hidalgo Vicario (2015) que “las nuevas tecnologías de la información y comunicación (TICs) constituyen aquellas herramientas y programas que tratan, administran, transmiten y comparten la información mediante soportes tecnológicos.”.

2.2.3.1. Internet.

Está catalogada como una TIC y uno de los derechos humanos digitales, siendo una “red de telecomunicaciones que utiliza líneas telefónicas, cables, satélites y conexiones inalámbricas para conectar computadoras y otros dispositivos a la World Wide Web” (akus.net, 2021).

Fernández Delpech (2016) manifiesta que el “internet es así mismo una red de redes de ordenadores instaladas en las diferentes partes del orbe e interconectadas entre sí mediante las líneas de comunicación de alta celeridad” (p. 5).

En los datos levantados por el INEC⁶ (2021) en el año 2020 el porcentaje de personas que utilizan internet a nivel nacional es del 70,7%. Las de personas que utilizan el internet en el área urbana asciende al 77,1% y el 56,9% en el área rural.

2.2.3.2. Computadora.

PC ACADEMIA (2020) lo define de la siguiente manera:

Una computadora (sinónimos: ordenador, computador) es un dispositivo electrónico conformado por múltiples componentes los cuales básicamente mediante programas procesan datos para transformarlos en información la cual es utilizada para múltiples fines y diversos alcances.

Es conocido que se encuentra integrada por el hardware y software: en esta parte intangible se encuentra conformada por datos e información y programas, por lo cual puede realizar tareas u operaciones para las que se encuentra programada.

El INEC (2021), menciona que en el año 2020 el porcentaje de personas que utilizan computadora descendió al 34.3%, por lo cual es importante mencionar que en la zona urbana se encuentra el uso en el 40.7%, mientras en la zona rural es del 20.5%.

2.2.3.2.1. Cámaras de vigilancia o cámara IP.

También denominada cámara de red, que, para formar una única unidad, para ser útil y necesaria se compone por una cámara y un ordenador.

En lo que respecta a las cámaras de videovigilancia, en su página el Servicio Integrado de Seguridad Ecu911 (2017), explicó que “Es un sistema tecnológico de vigilancia visual mediante cámaras de seguridad, que permiten la supervisión de la seguridad ciudadana en los lugares públicos donde están instaladas”.

Además determina que en Ecuador “existen alrededor de 6.500 cámaras de videovigilancia instaladas y operativas” (Servicio Integrado de Seguridad Ecu911, 2017).

2.2.3.3. Teléfonos inteligentes o smartphome.

Los smartphome o teléfonos inteligentes, es un dispositivo móvil que tiene funciones de cámara fotográfica de video, así como de una computadora como de un teléfono celular básico, con el cual se puede realizar llamadas o enviar mensaje de texto. Por las funciones incorporadas

⁶ Instituto Nacional de Estadística y Censo

se puede realizar videos y tomar fotografías, así mismo reproduce videos, fotografías, accede a internet, pudiendo utilizar las herramientas de las TICs como correos electrónicos, redes sociales y demás aplicaciones que puede acceder descargando. La característica más relevante es la utilización de sistemas operativos, por ser en la actualidad un ordenador personal y de fácil transportación, por ende, tiene una gran aceptación por los ciudadanos para su uso.

En Ecuador el 82 % de los ciudadanos utiliza el celular o teléfono inteligente, ya sea para reproducir y escuchar música, comunicarse por medio de llamadas o aplicaciones de redes sociales o buscar información en un navegador en internet (DW Akademie, 2016).

Los valores anteriores contrastan con lo que afirma el INEC; Instituto Nacional de Estadística y Censo (2021) que en el año dos mil veinte el porcentaje de personas que tiene al menos un teléfono celular activado incrementó 62,9% y en la zona urbana registraba el 67,7% y rural el 52,4%, la tendencia es al alza progresiva. De la población total el 47,4% su celular es inteligente o smartphone.

En Ecuador la empresa MENTINNO (2021), determinó que las líneas activas que utilizan un dispositivo móvil llegan al 83.6% es decir 14,88 millones de personas o ciudadanos.

2.2.4. Herramientas de las nuevas tecnologías de la información y comunicación (NTICs).

2.2.4.1. Redes Sociales.

Para Celaya (2011), “las redes sociales son lugares en Internet donde las personas publican y comparten todo tipo de información, personal y profesional, con terceras personas, conocidos y absolutos desconocidos”(p. 106), su difusión es masiva en la sociedad, ya que permite tener una comunicación colectiva, fluida y sobre todo al crear grupo de interes, formando comunidades.

El INEC (2021) determina que de total de la población de Ecuador el 44,6% de personas utilizan redes sociales desde su smartphone o teléfono inteligente.

2.2.4.2. Aplicaciones de mensajería.

También se las denomina apps o aplicaciones de mensajería o de chat, con las mismas se pueden llamar y hablar de forma instantánea, en las cuales se encuentra y se desarrolla actualizaciones de software como los bots, entre otras.

Según Gutiérrez-Rubí (2015), “las aplicaciones en los smartphones son una vía para aproximar personas con intereses comunes a través de la tecnología y resolver sus necesidades reales a partir de la propia iniciativa individual”.

Entre las aplicaciones de mensajería más conocidas tenemos a WhatsApp, Telegram, Signal, Facebook Messenger, entre otras.

Las aplicaciones de redes sociales, como de mensajería son usadas para captar datos, conforme nos explica DW Español (2021), que:

Al usar app de mensajería instantánea hay tres tipos de información que se transmiten, el primero son los datos de perfil, el nombre y el teléfono, estos son obligatorios, la foto y la información adicional del perfil son opcionales, el segundo es el contenido de los mensajes que enviamos y recibimos, lo que comunicamos a los demás pueden ser texto, hasta fotos, videos, emojis, audio, contacto o documentos, todas las apps de mensajería, Facebook incluida sostienen que no usan este tipo de información aun que pueden tener acceso a ella especialmente si habilitamos la copia en la nube, los metadatos son el tercer tipo de información que se comparten, no la vemos pero es necesaria para que el mensaje llegue a su destino, también contiene información sobre el uso de la app.

2.2.4.3. Aplicaciones o apps.

Las aplicaciones móviles son programas que se “puede descargar y al que puede acceder directamente desde su teléfono o desde algún otro aparato móvil – como por ejemplo una tablet o un reproductor MP3” (La Comisión Federal de Comercio. Información para consumidores, 2011), estas aplicaciones son fáciles de descargar, existiendo una aplicación para ello, llamado Play Store para dispositivos Android y para dispositivos iPhone, la aplicación de descarga tiene el nombre de App Store.

Existe innumerables aplicaciones, como aplicación de GPS que detectan la ubicación del usuario, al igual que Google Maps, una aplicación de mapas que brinda de la misma forma la ubicación del usuario.

Las redes sociales también tienen su aplicación, como Facebook, Tik Tok e Instagram. La red social Facebook detecta la ubicación de su usuario.

Es importante mencionar que hay aplicaciones relevantes las mismas que ayudan o contribuyen con la salud de su usuario, otras utilizadas para el deporte, un sin número, dependiente de la preferencia del usuario. Todas las aplicaciones generan datos de sus usuarios.

2.2.4.4. Software.

Son sistemas operativos, así como programas para el desempeño de procesadores de escritorio o móviles.

Un concepto más completo nos otorga GCFGlobal (2021), determinando que el “software es el conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento del equipo”, por ejemplo son aplicaciones, sistemas operativos, bots, navegadores web, etc.

2.2.4.5. Big Data.

La descripción más idónea es que el “Big Data no es otra cosa que la huella digital de todo lo que hacemos *online* u *offline*” (Norte Sosa, 2020, p. 76), también podemos mencionar la definición que nos brinda el publicista Barranco Fragoso (2012), determinando que el Big Data son las “enormes cantidades de datos (estructurados, no estructurados y semiestructurados)”.

En la línea de ideas manifiesta Sosa Escudero (2019), que el “big data/algoritmos es como herramienta de reconocimiento de patrones, en límite de la tecnología y lo social” (p. 47), la que se abastece de información proporcionada por aplicaciones, así como de plataformas como Google, Facebook, Instagram o WhatsApp, etc.

2.2.4.6. Inteligencia artificial.

Traigo al presente estudio una definición acorde:

“La inteligencia artificial es en sí la habilidad de un artefacto que presentar las mismas capacidades que los seres humanos, como la lógica, el aprendizaje, la creatividad y la capacidad de crear. La IA admite que los sistemas tecnológicos perciben su entorno, se relacionan con él, resolviendo problemas y actúan con un fin específico. El aparato recibe datos (ya acomodados o recopilados a través de sus propios sensores, como, por ejemplo una cámara), los procesa y responde a dichas imágenes. Los sistemas de IA son capaces de adaptar su comportamiento en cierto orden, como analizar los efectos de acciones previas y de trabajar de manera libre” (Parlamento Europeo, 2021).

2.2.4.7. Tratamiento de datos.

El «tratamiento» abarca una amplia gama de operaciones realizadas sobre los datos personales, que incluyen procedimientos manuales o automatizados. Estas son la obtención, investigación, colocación, estructuración, conservación, adaptación o modificación, como también la extracción, consulta, utilización, comunicación por transmisión, propagación o cualquier otra forma de habilitación de camino, cotejo o interconexión, limitación, supresión o destrucción de datos particulares. (Comisión Europea, 2016)

2.2.4.8. Cadena de bloques o Blockchain.

El blockchain es una tecnología innovadora que proporciona transparencia y sobre todo descentralización, siendo aplicable a todo tipo de transferencia o transacciones, es así que Francisco Bolaños et al., (2019) determina que “la cadena de bloques es una base de datos abierta, distribuida, transnacional, neutral y resistente a la censura que puede almacenar y transmitir todo tipo de datos incluyendo activos” (p. 97).

Entre las ventajas que nos proporciona la cadena de bloques nos menciona Francisco Bolaños et al., (2019) que “la información distribuida no puede ser controlada por un individuo o una organización”, así mismo “el registro de transacciones que se almacena en un ablockchain es público, por lo que puede ser visto y auditado por cualquier persona” (Francisco Bolaños et al, 2019, p. 100).

2.2.5. Ventaja del uso de las TICs.

El desarrollo de las TICs ha modificado nuestras vidas, por cuanto se desarrollaron para mejorar la comunicación y acortar distancias, influyendo en los mejores estándares de vida que se han logrado con el transcurso del tiempo.

Las TICs desde sus inicios, además de cumplir el rol de informar y entretener, han contribuido a mantener comunicada a la población, por ende, creando fuentes nuevas de trabajo, además son herramientas de gran ayuda ya que transmiten el conocimiento -de ahí el término sociedad del conocimiento-, además sirviendo para generar contenido con fines de distracción, creando así fuentes de ingresos para los usuarios que se dedican a ésta actividad.

Entre las ventajas más destacadas podemos mencionar es la que se encuentra en el área del conocimiento, es así que “el ámbito educativo no puede quedar al margen y debe incluirlas

como un método de abordar las diferentes materias pensando en unos alumnos que son nativos digitales” (UNIR, 2021).

El área laboral se encontró beneficiada por el desarrollo de las TICs, encontrándose en un proceso de desarrollo constante al ir adaptándose e incorporando tecnología para mejorar sus desempeño competitivo, siendo importante “el uso de los avances tecnológicos, ofrecen grandes ventajas a las empresas, en especial a las pequeñas y medianas empresas que son el nuevo centro de interés de las empresas tecnológicas y además nos ayudan a evitar problemas y conflictos” (Telefónica, 2021).

En época de pandemia -al encontrarnos en hacinamiento- y post pandemia, la tecnología ha ayudado a evitar la pérdida de trabajos y evitar que el área laboral se detenga en su totalidad, además es indiscutible que ha creado nuevas fuentes de trabajo en áreas tecnológicas en su mayoría.

El área de la salud también se ha beneficiado por las TICs y el desarrollo tecnológico, por cuanto es de implementación directa, desde “los registros informáticos supuso un gran avance en la gestión de una información tan sensible como el historial médico” (Clinic Cloud, 2019).

Una de las innovaciones en el área médica ha sido la telemedicina, la cual “se pueden usar para referirse a consultas médicas a través de videoconferencia, o la transmisión de datos de atención médica como electrocardiogramas (ECG)” (Clinic Cloud, 2019).

2.2.6. Desventaja del uso de las NTICs.

2.2.6.1. Contrato de términos y condiciones de uso.

Estos contratos lo encontramos al descargar una aplicación ya sea en Play Store de Google o App Store de Apple, o en las actuaciones de las aplicaciones que tienen los usuarios, las mismas que son recomendables leer para darse cuenta sobre el perjuicio que puede ocasionar las cláusulas, entre ellas tenemos:

Al instalar la app y aceptar los términos y condiciones de uso, les otorgamos una licencia de uso no exclusiva sobre el contenido que publicamos en la aplicación, también otorgamos el derecho a usar otros datos, como la ubicación exacta, las fotografías con el lugar de ubicación y su fecha de creación, entre otras (BBC NEWS, 2018).

2.2.6.2. Recolección de datos.

En la actualidad los datos son recursos valiosos con los cuales las empresas con modelos de negocio basados en datos, generan grandes ingresos, ya que los datos son apreciados en el área empresarial, hasta en la política, ya que son información de las personas.

El sector empresarial en su giro de negocios realiza procesos de análisis de datos, que según menciona Dejusticia (2020), que “se puede hacer análisis de mercado, determinar qué productos o servicios tienen mayor demanda, segmentar a las personas de acuerdo a sus gustos, ofrecer publicidad personalizada que responda a dichos gustos y muchas otras que benefician al mercado”.

El proceso de recolección de datos se generará en el desarrollo de tres pasos, según Dejusticia, son los siguientes, “a través de la entrega directa; recolectándolos a través de medios tecnológicos; y obteniéndolos de otras compañías que los recolectaron previamente a través de las modalidades anteriores” (2020).

El primer caso ocurre al acceder a una página web en la cual nos registramos o aceptamos cookies sin detenernos a leer los términos, o al crear un usuario en una aplicación móvil, en la cual se registra nuestra información en un perfil, creada la cuenta hay muchas opciones entre las cuales podemos agregar, como fotografías, además la ubicación del usuario es un dato que se genera, entre otros datos que generamos a diario, es así que hasta el dispositivo móvil cumple con la función de la recolección de datos del usuario.

En el segundo caso se genera cuando las empresas usan herramientas tecnológicas para recopilar de nuestros dispositivos información, utilizando el web tracking, proceso que se desarrolla usando “archivos de texto (cookies) o verificar las configuraciones y capacidades del dispositivo (fingerprint)” (Dejusticia, 2020).

Menciona Dejusticia (2020), que “estas técnicas permiten saber cuál es nuestro historial de búsqueda, cuánto tiempo permanecemos en la aplicación, cuál es la dirección IP del dispositivo desde el que nos conectamos y cuál es nuestra geolocalización, entre muchas otras cosas”.

En el tercer caso que es el medio de obtener datos a través de otras compañías ya sea al comprarlos o suscribir acuerdos de obtención o cruce de información como realiza la compañía

Facebook Inc o con su actual nombre Meta Platforms Inc., propietaria de las plataformas relevantes Facebook, WhatsApp e Instagram, entre otras. La información obtenida tan sólo de WhatsApp no genera dinero, lo que si es una fuente de ingreso para la empresa matriz son los datos privados y perfiles a partir de ellos, los que tienen miles de uso en los mercados (DW Español, 2021).

Menciona DW Español (2021), que la Unión Europea ha prohibido el intercambio de datos entre Facebook y WhatsApp, gracias al reglamento general de protección de datos, en la entrevista a la Dra. Jennifer King⁷, experta en privacidad, cree que la transferencia de datos puede tener graves consecuencias, ya que usan diversos datos para adaptar los contenidos a las distintas personas, en Estados Unidos vimos la controversia sobre la influencia de Facebook en las elecciones a través de publicidad electoral, estamos viendo que los algoritmos que usan para recomendar contenido en grupos de Facebook, han contribuido a radicalizar a los usuarios.

2.2.6.3. Compra y venta de datos personales.

La comercialización de los datos personales se ha vuelto normal en el área empresarial, estando expuesta nuestra información personal para cualquier situación, desde el acoso comercial, llegando hasta a producirse delitos.

En la página web de Softonic (2014), menciona que “Facebook comparte tus datos (nombre, lista de amigos e información pública) con muchos otros servicios como Bing, Pandora, TripAdvisor o Yelp de forma automática.

En lo que respecta a Amazon, esta empresa “puede vender tus datos a terceros en caso de que haya una transmisión de empresas. Los datos de los clientes son generalmente parte de los activos transferidos, pero estas operaciones siguen estando sujetas a los acuerdos de confidencialidad vigentes” (Softonic, 2014).

En Ecuador es fácil adquirir base de datos de los ciudadanos y empresas, es así que en sitios web como Mercado Libre, venden copias de archivos de base de datos, es así que en la investigación desarrollada a Data.ec por el diario Expreso (2021), menciona “que posee información a nivel de todo el Ecuador. Puede perfilar la base de datos según filtros o palabras

⁷ Dra. Jennifer King. Experta en protección de datos, Universidad de Stanford (California).

claves que el cliente indique y hasta obtener nuevos datos de acuerdo a los requerimientos del comprador”.

Las cifras en lo referente a transacciones de datos de las personas son alarmantes en Ecuador en la página web de Expreso (2021), se menciona que “el 90 % o más de transferencia (comercialización) que realizan las empresas son ilegales, porque en ningún momento el titular dio su consentimiento para que su información sea transferida a manos de terceros”.

2.3. Marco referencial.

2.3.1. Las tecnologías

Según el Diccionario de la lengua española (2019), tenemos dos definiciones útiles para la presente investigación donde se puede definir a las tecnologías como el “conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico.” y “conjunto de los instrumentos y procedimientos industriales de un determinado sector o producto.”.

2.3.2 TICs (Tecnologías de la Información y Comunicación)

Como definición de las TICS tenemos que son el conjunto de conocimientos que permiten el camino, producción, procedimiento y comunicación de información presentada en diferentes códigos (texto, imagen, sonido, ...). (Belloch Ortí, 2014, pp. 1-7). “Las TIC se basan en información digital contenida como 1s y 0s, y comprenden hardware, software y redes informáticas.” (Duncombe & Heeks, 1999, pp. 1-18).

2.3.3. Redes Sociales

Según la RAE; Real Academia Española (2020) se define a las redes sociales como: “Servicio de la sociedad de la información que ofrece a los usuarios una plataforma de comunicación a través de internet para que estos generen un perfil con sus datos personales, facilitando la creación de comunidades con base en criterios comunes y permitiendo la comunicación de sus usuarios, de modo que pueden interactuar mediante mensajes, compartir información, imágenes o videos, permitiendo que estas publicaciones sean accesibles de forma inmediata por todos los usuarios de su grupo”.

2.3.4. Big Data

Ricardo Barranco Fragoso, arquitecto de software, define al Big Data como la predisposición en el avance de la tecnología que ha abierto las puertas hacia un nuevo enfoque de intelecto y toma de disposiciones, la cual es monopolizada para describir enormes cantidades de identificaciones (estructurados, no estructurados y semis estructurados) que tomaría demasiado lapso y sería muy costoso cargarlos a un base de ficha relacional para su estudio. (Barranco Fragoso, 2012).

2.3.5 Inteligencia Artificial

La inteligencia artificial (IA) es la destreza de un aparato que presenta las mismas capacidades que los seres humanos, como la lógica, el aprendizaje, la creatividad y la capacidad de planear. La IA consiente que los sistemas tecnológicos perciban su ambiente, se relacionen con él, resuelvan problemas y actúen con un fin determinado. El aparato recibe datos (ya preparados o compendiados a través de sus propios sensores, como, por ejemplo, una cámara), los procesa y reconoce a ellos. Los sistemas de IA son capaces de adecuar su conducta en cierta medida, examinar los efectos de acciones previas y de trabajar de manera autónoma. (Parlamento Europeo, 2021, pp. 1-6)

2.3.6. Tratamiento de datos

Según el reglamento (UE) 2016/679 del parlamento europeo el «tratamiento» abarca una amplia gama de operaciones realizadas sobre los datos personales, que incluyen procedimientos manuales o automatizados. Estas son la obtención, investigación, organización, estructuración, subsistencia, adaptación o reforma, extracción, consulta, utilización, comunicación por transmisión, propagación o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción de datos personales. (Comisión Europea, 2016, p. 33)

2.3.7 Internet

La Real Academia Española define al internet como la red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación. (Real Academia Española, 2018). Según Elena de la cuadra el internet es una gran red internacional de ordenadores que permite, como todas las redes, compartir

recursos. Es decir: establecer vínculos comunicativos con millones de personas de todo el mundo, bien sea para fines académicos o de investigación, o personales (De La Cuadra, 1996, p. 35).

2.3.8. Videocámaras y video vigilancia

Podemos definir según la Real Academia Española a una videocámara en lugar público como al sistema de grabación de imágenes y sonidos en lugares públicos, abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública. (Real Academia Española, 2020).

La RAE también define a la videovigilancia como la vigilancia por medio de un sistema de cámaras, fijas o móviles. (Real Academia Española, 2020).

2.3.9. Teléfono inteligente o Smartphone

De acuerdo a la Real Academia Española el teléfono inteligente es un celular con pantalla táctil y con muchas de las prestaciones de una computadora. (Real Academia Española, 2020). El smartphone cuenta con todas las funciones básicas del celular (permite realizar llamadas telefónicas, enviar mensajes de texto, etc.) y le agrega características avanzadas (conexión a Internet, capacidad multimedia, pantalla táctil). (Pérez Porto & Merino, 2014).

2.3.10. Cadena de bloques o Blockchain.

La blockchain conforme Francisco Bolaños et al., (2019) es un “libro contable distribuido que almacena y mueve todo tipo de datos, incluyendo activos, en una estructura secuencial de bloques ordenados cronológicamente y relacionados matemáticamente entre sí. Los datos que contiene una cadena de bloques no pueden ser modificados, borrados o censurados sin el consenso de todos los participantes-nodos-de la red informática.” (p. 250).

2.4 Marco legal.

2.4.1. Teoría constitucional.

2.4.1.1. Derechos Humanos.

Para comprender el termino es importante definirlo, es así que “los derechos humanos son derechos universales, fundamentales, abstractos, válidos y morales” (R. Alexy, 2007, p. 237-248, como se citó en Bernal Pulido, 2018, p. 23).

Los derechos humanos son derechos inherentes a todos los seres humanos, sin distinción alguna de raza, sexo, nacionalidad, origen étnico, lengua, religión o cualquier otra condición. Entre los derechos humanos se incluyen el derecho a la vida y a la libertad; a no estar sometido ni a esclavitud ni a torturas; a la libertad de opinión y de expresión; a la educación y al trabajo, entre otros muchos. Estos derechos corresponden a todas las personas, sin discriminación alguna. (Naciones Unidas, s.f.)

2.4.1.2. Derechos Fundamentales.

La Real Academia Española se refiere a ellos como los derechos de una persona o de un ciudadano, que emanan de la dignidad humana, del libre desarrollo de la personalidad y de otros valores; se ejercen individualmente o de forma colectiva. Sus contenidos vinculan a todos los poderes públicos; su reconocimiento se establece en normas dotadas de supremacía material y su regulación y restricción vienen reservadas a la ley, que ha de respetar el contenido esencial. (Real Academia Española, 2020).

Para entender de una mejor manera, podemos instituir que “son derechos fundamentales o primordiales todos aquellos derechos subjetivos que corresponden universalmente a ‘todos’ los individuos” (Rentería Adrián, s.f, como se citó en Carbonell & Salazar, p. 121.)

Según Robert Alexy “los derechos fundamentales regulan con rango máximo (...), con máxima fuerza jurídica, objeto (...), máxima importancia (...), máxima indeterminación” (Carbonell, 2009, p. 32-33).

Es importante determinar la comparación con los derechos humanos, ya que “los derechos fundamentales se hallan regulados en la Constitución. De ello y de los principios *lex superior derogat legi inferiori* (...) se sigue que toda norma jurídica que los viole es inconstitucional y en consecuencia revocada por ser una regla general” (Carbonell, 2009, p. 33).

Es importante determinar que el reconocimiento en la legislación interna del país, expuesta en su Constitución, esto sirve para que:

Los derechos fundamentales se decide acerca de la estructura básica de la sociedad. (...) la garantía de la libertad de opinión, prensa radio y televisión (...) establece los pilares básicos del sistema de comunicación social. Otros derechos fundamentales han de mencionarse tan sólo con el fin de reconocer su contenido fundamental: (...) la protección de la vida y la integridad física (...) (Carbonell, 2009, p. 34-35).

Al efectuarse el desarrollo de los derechos fundamentales por parte de los ciudadanos, éste contribuye a que se configure el buen vivir, mismo que se puede hacer efecto en un ambiente democrático y de respeto a los derechos, la doctrina al respecto determina que:

Los derechos fundamentales son profundamente democráticos porque aseguran el desarrollo y la existencia de las personas gracias a la garantía de los derechos de libertad y de igualdad, capaces por lo general de mantener estable el procedimiento democrático, y por asegurar las condiciones para el funcionamiento del proceso democrático mediante la protección de la libertad de opinión, prensa, radiodifusión, reunión y asociación, así como el derecho del sufragio y otras libertades políticas (Carbonell, Neoconstitucionalismo (s), 2009, pág. 38)

Carbonell, (2007) establece cuales son los derechos fundamentales:

Según la teoría del derecho, la que los identifica con los derechos que están adscritos universalmente a todos en cuanto personas, o en cuanto a ciudadanos o personas con capacidad de obrar, y que son por tanto indivisibles e inalienables.

La segunda respuesta que ofrece el derecho positivo, es decir, la dogmática constitucional o internacional. Son derechos fundamentales, en el ordenamiento italiano o alemán, los derechos universales e individuales establecidos por el derecho positivo italiano o alemán. Son derechos fundamentales, en el ordenamiento internacional, los derechos universales e individuales establecidos en la Declaración universal de los derechos humanos de 1948, en los pactos internacionales de 1966 y en las demás convenciones internacionales sobre los derechos humanos.

La tercera respuesta (...) Deben estar garantizados como derechos fundamentales todos los derechos vitales cuya garantía es condición necesaria para la paz; el derecho a la vida y a la probidad de la persona, los derechos civiles y políticos, los derechos de libertad. (...) los derechos sociales para la supervivencia. (..) Igualdad en los derechos de libertad, que garantiza con valor todas las diferencias personales, (...) igualdad en los derechos sociales. Todos los derechos fundamentales son leyes del más débil e alternativa a la ley del más fuerte que regirá en su ausencia: derecho a la vida (...), derecho de inmunidad y de libertad (...), los derechos sociales, que son derechos a la supervivencia contra la ley de quien es más fuerte social y económicamente. (p. 73-75)

2.4.1.3. Derecho a la intimidad personal y familiar.

Debemos definir este derecho, para lo cual tomaremos las palabras de Fernández Delpech:

El derecho a la intimidad es un derecho personalísimo al que se lo ha definido como el derecho que tienen los individuos de poder excluir a las demás personas del conocimiento de su vida personal, es decir de sus sentimientos y comportamientos, y que les permite determinar por su cuenta cómo y en qué medida las informaciones que les atañen pueden ser comunicadas a otras personas. (Fernández Delpech, 2014, p. 327)

Este derecho fundamental es de suma importancia para alcanzar una calidad mínima de vida, con el cual poder desarrollar capacidades plenas sin sentirse limitado en la sociedad, es así que:

El derecho a la intimidad es reconocido e idéntico precepto constitucional como derecho fundamental, gozando de tutela tanto de ámbito personal como familiar, estando justificada por la pretensión de preservar y, con ello, dotar de protección a un ámbito particular de la persona, para así hacerlo intocable para el resto de sujetos, conllevando el reconocimiento de un espacio propio e impenetrable sobre el cual no puede transmitirse al exterior dato alguno sin el consentimiento del titular. (de la Iglesia Prado, 2018, p. 205)

El derecho fundamental a la privacidad y a la vigilancia masiva, a medida que avanzan las tecnologías que facilitan la vigilancia estatal de las comunicaciones, los estados están fallando en garantizar que las leyes y regulaciones relacionadas con la vigilancia de las

comunicaciones estén en consonancia con el derecho internacional de los derechos humanos y protejan adecuadamente los derechos a la intimidad y a la libertad de expresión. (FERNANDEZ, 2014)

Al adoptar una nueva técnica de vigilancia de las comunicaciones o al ampliar el alcance con el que este pueda determinar, si la información que podría adquirir cae en el ámbito de la “información protegida”, y deberían someterse al escrutinio judicial u otro mecanismo de control democrático. Puesto que el monitoreo generalizado o sistema tiene la capacidad de revelar información privada, y este su vez eleve la vigilancia de la información no protegida a un nivel invasivo que exija a su vez una mayor información según el criterio del autor (FERNANDEZ, 2014).

El derecho a la intimidad personal y familiar, se encuentra examinado y reconocido en el numeral veinte del artículo sesenta y seis de la constitución de la república del Ecuador.

El presente derecho lo encontramos reconocido en el tratado internacional como la, convención americana sobre los derechos humanos: “Pacto de San José de Costa Rica”, en su numeral dos del artículo once, el que establece que “Nadie puede ser centro de indiscreciones arbitrarias o injustas en su vida privada, en la de su familia, en su morada o en su correspondencia, ni de ataques ilegales a su recato o reputación” (Estados Americanos, 1969).

2.4.1.4. Derecho a la protección de datos de carácter personal.

El estado ecuatoriano reconoce y garantiza el derecho a la defensa de datos de carácter propio, el mismo que se encuentra contemplado en el numeral diecinueve del artículo sesenta y seis de la constitución. El cual establece lo siguiente:

El derecho a la protección de datos de carácter propio, que a su vez incluye el acceso y la decisión sobre búsqueda y datos de este carácter, así como su correspondiente amparo. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la permisión del titular o el mandato de la ley. (Asamblea Nacional del Ecuador, 2008)

2.4.1.5. Derecho a la inviolabilidad y al secreto de la correspondencia física y virtual.

Este derecho se enmarca en el derecho a la intimidad, rechazando a la intromisión en la correspondencia ya sea física o en los medios digitales que en la actualidad se usan, cómo el correo electrónico.

El presente derecho lo encontramos reconocido en el numeral veintiuno del artículo sesenta y seis de la carta magna, el mismo que se lo transcribe taxativamente a continuación:

El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ya que ésta su vez no podrá ser retenida, abierta ni examinada, excepto en los asuntos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de información. (Asamblea Nacional del Ecuador, 2008)

Reconoce a este derecho el tratado internacional como es la convención americana sobre los derechos humanos “Pacto de San José de Costa Rica”, en su numeral dos del artículo once, el que determina que “Nadie puede ser centro de injerencias arbitrarias o injustas en su vida privada, en la de su familia, en su morada o en su correspondencia, ni de arremetas ilegales a su pudor o reputación” (Estados Americanos, 1969).

2.4.1.6. Derecho a la libertad de información.

El derecho a la libertad de información lo encontramos desarrollado en los numeral uno y dos del artículo dieciocho de la constitución del Ecuador, el que determina lo siguiente:

Todos los seres humanos, en forma individual o colectiva, tienen derecho a: 1. Escudriñar, recibir, intercambiar, originar y difundir información veraz, verificada, pertinente, contextualizada, plural, sin censura previa acerca de los hechos, sucesos y procesos de interés general, y con compromiso ulterior. 2. Acceder libremente a la averiguación generada en entidades públicas, o en las privadas que manejen fondos del Estado o ejecuten funciones públicas. No existirá discreción de información excepto en los casos expresamente establecidos en la legislación. En caso de violación a los derechos humanos, ninguna entidad pública entorpecerá la información. (Asamblea Nacional del Ecuador, 2008)

2.4.1.7. Derecho al honor y buen nombre.

Debe de dejarse establecido, que el derecho al honor es independiente del derecho a la intimidad personal.

Un concepto apropiado es el que nos proporciona Garriga Domínguez:

Es el derecho que tiene todo ser humano a ser tratado de manera compatible con su dignidad, que se manifiesta de forma clara y directa en la estimación que él siente por sí mismo y que espera de los demás. Es un derecho considerado desde siempre inherente a la persona. (2016, p. 83)

Nuestra legislación lo contempla y reconoce éste derecho, encontrándose establecido en el numeral dieciocho del artículo sesenta y seis de la carta magna, determinando que “Todas las personas, de manera individual o colectiva, tienen derecho a: el derecho al decoro y al buen nombre. La ley protegerá la imagen y la voz del prójimo” (Asamblea Nacional del Ecuador, 2008).

2.4.1.8. Derecho a la imagen.

Este derecho es catalogado como derecho fundamental del ser humano, siendo autónomo y gozando de protección independiente.

Establece Garriga Domínguez que es un derecho “de personalidad derivados de la dignidad de la persona y orientados a proteger su patrimonio moral” (2016, p. 87), guardando relación con el derecho al honor y el derecho a intimidad.

Lo encontramos reconocido en la parte final del numeral dieciocho del artículo sesenta y seis de la constitución de la república del Ecuador.

2.4.1.9. Derecho a libertad de Expresión.

La libertad de expresión es un derecho humano, reconocido y contemplado en la Declaración Universal de los Derechos Humanos el mismo que contempla que los individuos tienen la libertad de opinar y expresarse, sin ser molestado o investigado por esas opiniones, fundamento para consolidar las democracias.

La libertad de expresión es fundamental en los regímenes democráticos, en este orden de ideas los medios de comunicación juegan un papel importante, y en el presente siglo la irrupción

del internet que se ha “convertido en el epicentro de las comunicaciones, y a través de ella de la transferencia de la información, con la particularidad de su masividad, rapidez, y ausencia de límites territoriales” (Fernández Delpech, 2014, p. 158).

Si bien el internet con los dispositivos móviles son herramientas con las cuales ejercer el presente derecho, pero también puede incidir en reproducir mensajes que carezcan de fundamento o siendo elaborados previamente para incidir en la opinión y pensamiento de las personas, con las famosas noticias falsas, hasta llevar a los individuos a cometer actos que atenten contra otros derechos.

El derecho a la libertad de expresión se encuentra reconocido en nuestra constitución en el numeral seis del artículo sesenta y seis de la constitución del Ecuador.

2.4.1.10. Derecho a la protesta.

El derecho constitucional a “la protesta es una forma de acción individual o colectiva dirigida a expresar ideas, visiones o valores de disenso, oposición o reivindicación” (Comisión Interamericana de Derechos Humanos (CIDH), 2019, p. 5).

En la actualidad, los ciudadanos utilizan el internet para diversas actividades y una de ellas, es la de “asociarse y reunirse que las personas adquieren en la era digital y que potencia, a su vez, la plena realización y el goce de otros derechos civiles, políticos, económicos, sociales y culturales” (Comisión Interamericana de Derechos Humanos (CIDH), 2019, p. 97), siendo un mecanismo de acceso, de costo bajo y por ende ideal para organizarse y tomar decisiones en lo que respecta a sus derechos, muy útil en tiempo de pandemia de la gripe china o COVID-19.

Siendo en la actualidad utilizada para “el control y la denuncia de violaciones a los derechos humanos durante manifestaciones y reuniones” (Comisión Interamericana de Derechos Humanos (CIDH), 2019, p. 97).

“El derecho a asociarse, reunirse y manifestarse en forma libre y voluntaria” (Asamblea Nacional del Ecuador, 2008), lo encontramos en nuestra constitución en el numeral trece del artículo sesenta y seis.

2.4.1.11. Derecho a la libertad de tránsito y libre movilidad.

Este derecho consiste en entrar al país, permanecer, transitar y salir sin ninguna limitación, la única restricción es la emanada de una decisión de autoridad judicial competente.

El derecho al tránsito dependiendo al caso particular se podría encontrar correlacionado con los derechos de reunión, libertad de expresión y de protesta, posterior al desarrollo de éstos últimos, podría verse limitado al tomarse represalias por haber ejercido los mismos, generándose la violación de derechos.

La forma que en la actualidad se ve afectado este derecho, es por la tecnología, ya que, al encontrarse instaladas cámaras de vigilancia en las áreas públicas, es fácil la identificación de las personas que ejercen su derecho a la protesta, pudiendo llegar hacer perseguidos políticos, viéndose limitado sus derechos.

Nuestra carta magna reconoce este derecho humano en su numeral catorce del artículo sesenta y seis: “El derecho a transitar libremente por el territorio nacional (...)” (Asamblea Nacional del Ecuador, 2008).

2.4.1.12. Derecho al olvido digital.

El concepto que nos proporciona Terwangne, deja establecido que “el derecho al olvido, o también llamado el derecho a ser olvidado, es el derecho de las personas físicas a hacer que se les suprima la información sobre ellas después de un período de tiempo determinado” (2012, p. 53).

También se puede mencionar que es el “derecho a solicitar, en definitiva, que en determinados casos se cancelen datos personales que circulan por internet ante el riesgo que ello supone en la vulneración de los derechos de la personalidad (particularmente, los derechos al honor e intimidad)” (Murga Fernández, 2018, p. 223).

Es importante destacar que éste derecho consta en la legislación del parlamento europeo, no contemplado en la novísima ley orgánica de protección de datos personales del Ecuador.

2.4.1.13. Garantía Jurisdiccional de Acción de Habeas Data.

Fernández Delpech, manifiesta que “la acción de hábeas data constituye una clara garantía constitucional que atiende a la protección de los derechos de los titulares de datos

personales, que se consideren afectados por el manejo incorrecto e indiscriminado de sus datos” (2016, p. 363), por parte de las compañías privadas y del propio estado.

Es importante destacar lo que nos aporta la Dra. Aida García Berni a través de la página web de Derecho Ecuador, estableciendo que “la doctrina y la legislación latinoamericanas tienen diferentes enfoques sobre la garantía que protege esta acción, pero es más generalizada la idea de que el hábeas data protege el derecho a la intimidad, y el derecho al pudor y buena reputación” (2005), la que se vería afectada por medios tecnológicos que recopilan datos o información personal.

Nuestra legislación contempla la presente garantía en el artículo noventa y dos de la constitución, el mismo que es menester transcribirlo:

Todos los seres humanos, por sus propios derechos o como representante legitimado para el efecto, gozarán del derecho a conocer de la existencia y a suscribirse a los documentos, datos genéticos, bancos o registros de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, también tendrá derecho a conocer el uso que se haga de cada uno de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

El sujeto titular de los datos podrá requerir al responsable el acceso sin costo al archivo, así como la modernización de los datos, su rectificación, eliminación o revocación. En el caso de datos sensibles, cuyo archivo deberá estar acreditado por la ley o por la persona titular, se requerirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados. (Asamblea Nacional del Ecuador, 2008)

Esta garantía jurisdiccional tiene la capacidad de resguardar nuestro derecho a la honra y buena popularidad. Su naturaleza es para facilitar el acceso a los datos que conste del residente, ya sea públicas o privadas, pudiendo requerir “la actualización de los datos, su rectificación, como también eliminación o anulación” (Asamblea Nacional del Ecuador, 2008).

2.4.2. Legislación de la Unión Europea con respecto a la protección de datos personales.

La Carta de Derechos Fundamentales de la Unión Europea, contempla en su artículo ocho que “toda persona tiene el derecho a la protección de los datos de perfil personal que le conciernan” (Parlamento Europeo, el Consejo y la Comisión, 2012).

La Unión Europea cuenta con el derecho al olvido que se encuentra contemplado en el “Reglamento (UE) 2016-679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 el cual es relativo a la protección de las personas físicas en lo que respecta al procedimiento de datos personales y al libre movimiento de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)” (Murga Fernández, 2018)

El reglamento determina la normativa sobre la protección de datos personales y las normas bajo las cuales puede circular los datos, es importante por cuando su aplicación no es sólo tiene su alcance dentro de su territorio, sino en el lugar que la empresa trate los datos, además de ello limita la transferencia de los datos, siendo la norma estricta al respecto, prohibiéndose la venta de datos personales y demás regulaciones estrictas.

Con esta normativa legal, la Unión Europea ha prohibido el intercambio de datos entre Facebook y WhatsApp, gracias al reglamento general de protección de datos.

2.4.3. Instrumentos internacionales.

2.4.3.1. Declaración Universal de Derechos Humanos (DUDH).

Esta declaración se adoptada y se proclamó por la Asamblea General en su resolución 217 A (III), de 10 de diciembre de 1948. (Naciones Unidas, 1948), en la misma se reconoce derechos como el derecho a la intimidad personal y a la familiar, el derecho a la inviolabilidad y al secreto de la comunicación física y virtual, el derecho al honor y buen nombre en su artículo doce, el derecho a la libertad de tránsito en su artículo trece, el derecho a la libertad de expresión y de información, contemplado en el artículo diecinueve, así mismo reconoce el derecho a libertad de reunión y de asociación pacífica en su artículo veinte, entre otros.

2.4.3.2. Convención Americana sobre los Derechos Humanos. “Pacto San José de Costa Rica”.

La presente convención desarrolla los derechos como el derecho a la honra y a la dignidad, así como las impertinencias arbitrarias o abusivas en su vida íntima, en la de su familia

o en su correspondencia, también denominados, el derecho a la intimidad personal y familia e inviolabilidad y al secreto de correspondencia en su artículo once. El derecho a la libertad de pensamiento y expresión se encuentra establecido en el artículo trece. Los artículos quince y dieciséis desarrollan derechos como el de reunión y libre asociación.

2.4.3.3. Pacto Internacional de Derechos Civiles y Políticos.

El presente pacto contempla el derecho a la libre movilidad y tránsito en su artículo doce. El derecho a la intimidad y la inviolabilidad de correspondencia se encuentra reconocido en el artículo diecisiete. El derecho a la libertad de expresión y el respeto a la reputación se encuentra contemplado en el artículo diecinueve. El ejercicio al derecho de reunión pacífica y el derecho a asociarse libremente, se encuentra contemplado en los artículos veintiuno y veintidós.

2.4.3.4. Declaración de Derechos del Ciberespacio.

En la página web del Observatorio Iberoamericano de Protección de Datos se encuentra la Declaración de Derechos del Ciberespacio, este documento ve la luz, luego de un análisis riguroso de la sociedad de la información y del conocimiento, por “el prestigioso catedrático Español, Emilo Suñé Llinás el 06 de octubre del 2008 (...) en el año 2012 introdujo una modificación en su artículo primero” (Fernández Delpech, 2016, p. 15).

Ésta declaración es emitida por un catedrático que preocupado por el ejercicio de derechos en el ciberespacio, realizó una análisis riguroso que corresponde a los derechos que pisiblemente se podrían ver afectados por la actividad la web, los mismos que deben ser protegidos. No es un documento oficial acogido por estados como normativa, pero si es de gran aporte para la comunidad académica.

2.4.3.5. Derecho Humano al Acceso a Internet.

En el trigésimo segundo período de sesiones del Consejo de Derechos Humanos, la asamblea general de las naciones unidad, emite la resolución no vinculante exhortando a los estados miembros sobre la “promoción, protección y disfrute de los derechos humanos en Internet” (Naciones Unidas, 2016), por ende, considerándose al internet derecho humano, ya que al prohibir o impedir su acceso se considerará violación a los derechos humanos.

La Comisión Interamericana de Derechos Humanos (CIDH) establece que el “internet actualmente constituye una herramienta fundamental de comunicación que permite a las

personas vincularse y conectarse de manera ágil, veloz y efectiva, y es considerada una herramienta con un potencial único para el ejercicio de la libertad de expresión” (2019, p. 97).

2.4.4. Sistema Interamericano de Protección de los Derechos Humanos (SIDH).

La definición digna de estudio es la que nos otorga la ONU, destacando que el:

El Sistema Interamericano de Protección de los Derechos Humanos (SIDH) es el conjunto de normas sustantivas y procesales, organismos y mecanismos de denuncia que, en el marco de la Organización de Estados Americanos (OEA), cumplen la función de promover y proteger los derechos humanos universales en América. (2015).

2.4.4.1. Comisión Interamericana de Derechos Humanos.

“La CIDH es un órgano principal y autónomo de la Organización de los Estados Americanos (OEA) encargado de la promoción y protección de los derechos humanos en el continente americano” (OEA, 2021).

La Carta de la Organización de Estados Americanos (OE) y de la Convención Americana sobre Derechos Humanos, otorga el mandato a la Comisión Interamericana para promover tanto la observancia, cómo la defensa de los derechos humanos en los países de la región, emitiendo informes en defensa de los derechos, pudiendo presentar casos de violaciones de los derechos ante la Corte Interamericana de Derechos Humanos.

2.4.4.2. Corte Interamericana de Derechos Humanos

Maqueo Ramírez, et al. (2017) afirma que:

Hasta el momento la Corte Interamericana de Derechos Humanos (en adelante, CIDH) no se ha pronunciado de manera específica en ningún caso respecto del derecho a la protección de datos personales, a pesar de que un gran número de países sujetos a su jurisdicción lo contemplan dentro de su propio derecho interno con el carácter de derecho humano.

Por lo cual queda decir que el desarrollo del derecho a la protección de datos personales se desarrolla con mayor interés en Europa “a partir de la propia construcción expansiva del derecho a la vida privada hasta el reconocimiento de su propia autonomía” (Maqueo Ramírez, et al. 2017)

2.4.5. Pronunciamento legal en países Hispanoamericanos.

2.4.5.1. Caso Fierro Vs Google Inc. Sentencia T-063A/17. Corte Constitucional de Colombia.

El caso se desprende de la acción de tutela interpuesta por John William Fierro Caicedo, contra Google Inc. y otros, dentro del expediente T-5.771.452.

El presente caso ventilado en la Corte Constitucional de la República de Colombia, desarrolla el “derecho a la intimidad, a la honra y al buen nombre en página web o sitio de internet-Vulneración por parte de Google Inc. al haberse negado a eliminar un blog anónimo con contenido difamatorio, deshonroso y calumnioso contra el demandante y su empresa” (Corte Constitucional República de Colombia, 2018).

En su análisis revisa y se pronuncia sobre los derechos a la intimidad personal, a la honra y al buen nombre, derecho a la dignidad humana, dejando establecido los límites de la libertad de expresión e información, así como las diferencias entre derecho a la libertad de información y derecho de opinión, libertad de expresión en el internet.

En la Sentencia T-063A/17 dictada de fecha 03 de febrero del 2017 se resuelve amparar los derechos invocados por el accionante de la causa y para evitar la vulneración de estos derechos la Corte Constitucional República de Colombia (2018) exhorta:

Al Ministerio de Tecnologías de la Información y las Comunicaciones para que establezca una regulación nacional con miras a lograr la protección de los derechos de los usuarios de Internet, especialmente en lo que tiene que ver con publicaciones que atenten contra el honor de las personas en Internet.

Pero ocurre un caso particular, ya que dentro del auto 285/18, dictado de fecha 09 de mayo del 2018, “declara la nulidad de la presente providencia por violar el debido proceso, en virtud a la omisión de estudio de asuntos de relevancia constitucional” (Corte Constitucional República de Colombia, 2018).

Los estudios que se omitieron sobre asuntos de relevancia constitucional son “la prohibición de la censura, y la diferenciación entre el autor de las afirmaciones y quienes proveen el alojamiento de la información en Internet” (Global Freedom of Expression Columbia University, 2021).

Es decir, que la orden impuesta por la Corte Constitucional a Google del monitoreo constantemente el contenido de su blog sin una autorización judicial previa constituye una forma de censura que vulnera el derecho a la libertad de expresión y de información (Global Freedom of Expression Columbia University, 2021).

2.4.6. Normativas jurídicas que rige la protección de datos en el Ecuador.

Normativa	Artículos	Descripción
Constitución del Ecuador del 2008.	Art 16, num. 2.	Todos los seres humanos, en forma individual o colectiva, tienen el derecho a: 2. El acceso universal a las tecnologías de información y comunicación.
	Art. 66, num. 19	El derecho a la protección de datos de carácter privado, que incluye el acceso y la disposición sobre información y datos de este carácter, así como su correspondiente amparo. La recolección, registro, procesamiento, distribución o propagación de estos datos o información requerirán la autorización del titular o el mandato de la ley.
	Art. 66, num. 20	Garantizar el derecho a la intimidad de la persona y la familiar.
Ley Orgánica de Transparencia y Acceso a la Información Pública	Art. 2, literal d.	Garantizar el amparo de la información personal en poder del sector público y/o privado.
Código de la niñez y adolescencia	Art. 53.	Derecho a la privacidad y a la inviolabilidad del hogar y las formas de comunicación. - Sin perjuicio de la natural vigilancia de los padres y maestros, los niños, niñas y adolescentes tienen derecho a que se respete la intimidad de su vida privada y familiar; y la privacidad e inviolabilidad de su domicilio, correspondencia y comunicaciones telefónicas y electrónicas, de conformidad con la ley. Se prohíbe las injerencias arbitrarias o ilegales en su vida privada.
Ley Orgánica del Sistema Nacional de Registro de Datos Públicos	Art. 4.	Responsabilidad de la información. - Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro dispongan bases o registros de datos públicos, son responsables de la rectitud, amparo y control de las investigaciones y bases de datos a su cargo. Dichas instituciones se reconocerán por la veracidad, realidad, custodia y debida conservación de las búsquedas. La responsabilidad sobre la veracidad y autenticidad de los datos reconocidos, es privilegio de la o el declarante cuando esta o este provee toda la información. Las personas afectadas por información falsa o imprecisa, difundida o certificada por registradoras o registradores, tendrán derecho a las indemnizaciones correspondientes, previo el ejercicio de la respectiva acción legal. La Dirección Nacional de Registros Públicos establecerá los casos en los que deba rendirse

caución.

	Art. 6	Accesibilidad y confidencialidad. - (Sustituido por el lit. f del num. 1 de la Disp. Reformatoria Segunda de la Ley s/n, R.O. 459-5S, 26-V-2021).- Son confidenciales los datos de carácter personal. El acceso a estos datos, solo será posible cuando quien los requiera se encuentre debidamente legitimado, conforme a los parámetros previstos en la Ley Orgánica de Protección de Datos Personales, su respectivo reglamento y demás normativa emitida por la Autoridad de Protección de Datos Personales. Al amparo de esta Ley, para acceder a la información sobre el patrimonio de las personas cualquier solicitante deberá justificar y motivar su requerimiento, declarar el uso que hará del mismo y consignar sus datos básicos de identidad, tales como nombres y apellidos completos, número del documento de identidad o ciudadanía, dirección domiciliaria y los demás datos que mediante el respectivo reglamento se determinen. Un uso distinto al declarado dará lugar a la determinación de responsabilidades, sin perjuicio de las acciones legales que el titular de la información pueda ejercer. La directora o director nacional de Registros Públicos, definirá los demás datos que integran el sistema nacional y el tipo de reserva y accesibilidad.
Ley de Comercio Electrónico, Firmas y Mensajes de Datos.	Art. 5.	Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia.
	Art. 9.	(Derogado por la Disp. Reformatoria Primera de la Ley s/n, R.O. 459-5S, 26-V-2021).
	Art. 32.	Protección de datos por parte de las entidades de certificación de información acreditadas.- Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta ley.

Código Orgánico Integral Penal (COIP)	Art. 178.	<p>Violación a la intimidad.- La persona que, sin contar con el aprobación o la autorización legal, acceda, intercepte, reconozca, detenga, grabe, transcriba, difunda o publique datos personales, mensajes de datos, voz, audio y representación, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será penada con pena privativa de libertad de uno a tres años.</p> <p>No son aplicables estas reglas para la persona que divulgue grabaciones de audio y vídeo en las que interviene en persona, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.</p>
	Art. 182.	<p>DELITO CONTRA EL DERECHO AL HONOR Y BUEN NOMBRE</p> <p>Calumnia.- La persona que, por cualquier contorno, realice una falsa imputación de un delito en contra de otra, será sancionada con penalidad privativa de libertad de seis meses a dos años.</p> <p>No constituyen calumnia los pronunciamientos vertidos ante autoridades, jueces y tribunales, cuando las imputaciones se hubieren hecho en razón de la protección de la causa. No será responsable de las calumnias quien probare la veracidad de las imputaciones. Sin embargo, en ningún caso se admitirá experimento sobre la imputación de un delito que hubiere sido objeto de una sentencia ratificatoria de la inocencia del procesado, de sobreseimiento o archivo.</p> <p>No habrá lugar a responsabilidad penal si el autor de calumnias, se revocare voluntariamente antes de proferirse sentencia ejecutoriada, siempre que la publicación de la retractación se haga a costa del comprometido, se cumpla en el mismo medio y con las mismas características en que se difundió la imputación. La retractación no constituye una forma de aceptación de culpabilidad.</p>
	Art. 183.	<p>Restricción a la libertad de expresión.- La persona que, por medios violentos, coarte el derecho a la libertad de expresión, será castigada con pena privativa de libertad de seis meses a dos años.</p>
	Art. 190.	<p>Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será castigada con pena privativa de libertad de uno a tres años.</p> <p>La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.</p>

	Art. 229.	<p>Revelación ilegal de base de datos.- El individuo que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, registros, bases de datos o medios semejantes, a través o administradas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la infracción del secreto, la intimidad y la privacidad de las personas, será castigada con pena privativa de libertad de uno a tres años.</p> <p>Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.</p>
Ley Orgánica de Protección de datos personales.	Art. 1.	<p>El objeto y finalidad de la presente ley es certificar el ejercicio del derecho a la protección de datos personales, que incluye la dirección y decisión sobre información y datos de este carácter, así como su correspondiente amparo. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela.</p>

Tabla 1. Normativas jurídicas que rige la protección de datos en el Ecuador.

Elaborado por: Omar Altamirano Villena (2021)

Entre las normativas jurídicas que rige la protección de datos en el Ecuador y con las cuales podemos hacer prevalecer nuestros derechos involucrados, encontramos a las siguientes:

1. Constitución de la república del Ecuador del 2008.
2. Ley Orgánica de Transparencia y Acceso a la Información Pública.
3. Código Orgánico de la niñez y adolescencia
4. Ley Orgánica del Sistema Nacional de Registro de datos Públicos.
5. Ley de Comercio Electrónico, Firmas y Mensajes de Datos.
6. Código Orgánico Integral Penal (COIP)
7. Ley Orgánica de Protección de Datos Personales.

2.4.7. Pronunciamiento de la Corte Constitucional del Ecuador.

2.4.7.1. Sentencia N 2064-14-EP/21. Caso N 2064-14-EP

Dentro de la presente acción de protección se dicta la sentencia en la que se declara la violación al derecho a la protección de datos personales y autodeterminación informativa, a la imagen y buen nombre e intimidad, al tratar la sentencia de segundo nivel que resolvió revocar la decisión de primer nivel y declarar sin lugar la acción de habeas data planteado en contra de una persona natural que poseía fotografías íntimas y personales de la actora (Corte Constitucional del Ecuador, 2021).

Dentro de la sentencia se entra a analizar temas como el alcance del concepto de dato personal, el consentimiento del titular para el tratamiento de datos personales, el derecho a la intimidad, entre otros derechos conexos al tema.

2.4.7.2. Sentencia No. 182-15-SEP-CC. CASO 1493-10-EP.

La presente sentencia se desprende de Acción Extraordinaria de Protección 1493-10-EP, propuesta por:

Leandro Rufino Ullón Rodríguez y Walter Eduardo Armijos Orellana, Alcalde y Procurador Síndico del GADM Gobierno Municipal del cantón Mocache respectivamente, presentaron acción extraordinaria de protección en contra de la sentencia impuesta el 27 de agosto de 2010, por la Sala Penal, Colutorio y Tránsito de la Corte Provincial de Justicia de Los Ríos, dentro de la acción de hábeas data presentada por el señor Emilio Vicente Díaz Terán en contra de la Municipalidad de Mocache. (Corte Constitucional del Ecuador, 2015)

La resolución de la sentencia es aceptar la acción y declarar la vulneración del derecho a la seguridad jurídica, dejando sin efecto la sentencia de primer y segundo nivel materia de la presente acción, y en virtud de sus competencias efectúa la interpretación del artículo cincuenta de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, en los siguientes términos:

Las competencias establecidas en el artículo cuatrocientos treinta y seis numerales uno y tres de la Constitución de la República, la Corte Constitucional efectúa la interpretación conforme y condicionada con efectos erga omnes del artículo cincuenta de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, en consecuencia se deberá entender de la siguiente manera: La persona natural o jurídica pública o privada requerida deberá responder a la solicitud efectuada por el titular de la información personal en un plazo razonable que permita de mejor manera la satisfacción del derecho, que dependerá de la cantidad de la información requerida, del tipo de pedido y de la propia conducta de la persona natural o jurídica pública o privada que posea la administración de los datos requeridos.; La calificación de la razonabilidad de este plazo deberá ser realizada por el juez competente en la acción de Hábeas Data, al momento de la calificación de la demanda de esta garantía jurisdiccional.; La falta de contestación de

la persona natural o jurídica pública o privada que tenga bajo su administración los datos de una persona, sobre la solicitud que su titular efectúe respecto del acceso a los instrumentos, datos genéticos, bancos o archivos de datos personales e informes en poder de éstas, o respecto de la solicitud de actualización, rectificación, eliminación o anulación de datos que fueren erróneos o afecten los derechos de estos titulares, será considerada como negativa tácita por lo que se enmarcará en los presupuestos de la acción de Hábeas Data contenidos en los numerales uno y dos del artículo cincuenta de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. (Corte Constitucional del Ecuador, 2015)

Además, considera pertinente la emisión de reglas jurisprudenciales con efecto erga omnes, para la acción constitucional de hábeas data, en los siguientes términos:

De igual forma, esta Corte Constitucional, investida de las atribuciones contempladas en el artículo cuatrocientos treinta y seis numerales uno y seis de la Constitución de la República, respecto de la naturaleza, contenido y alcance de la acción constitucional de hábeas data, considera pertinente la emisión de las siguientes reglas jurisprudenciales con efecto erga omnes; Naturaleza: La acción de hábeas data es la garantía constitucional que le permite a la persona natural o jurídica, acceder a la información que sobre sí misma reposa en un registro o banco de datos de carácter público o privado, a fin de conocer el contenido de la misma y de ser el caso, exigir su actualización, rectificación, eliminación o anulación cuando aquella información le causan algún tipo de perjuicio, a efectos de salvaguardar su derecho a la intimidad personal y familiar.; Contenido: La acción constitucional de hábeas data, protegerá el derecho a la intimidad, la honra, la integridad psicológica de la persona, puesto que no toda la información relativa a estos tiene el carácter de pública y por tanto de divulgable en forma libre. En efecto, existen asuntos relativos a su familia, sus creencias religiosas y espirituales, su filiación política, su orientación sexual, entre otras, que en caso de ser divulgadas de forma inadecuada e inoportuna podrían ocasionarle serios perjuicios en la esfera personal.; Alcance: La acción constitucional de hábeas data tiene lineamientos determinados que deben ser observados por quien ejerce la legitimación activa de la misma, quien de escritura especial, al redactar su pretensión deberá estructurar su pedido de conformidad con los medidas establecidos para el efecto en la Constitución, en la Ley Orgánica de Garantías

Jurisdiccionales y Control Constitucional y en la jurisprudencia vinculante expresada por este Organismo sobre dicha acción lo cual coadyuvará, en primer lugar a que la gestión no se desnaturalice y en segunda parte, a que la dirección de justicia constitucional sea más ágil y eficaz para el fin que se persigue. (Corte Constitucional del Ecuador, 2015)

Esta sentencia enriquece la jurisprudencia constitucional por la interpretación y emisión de reglas para la garantía jurisdiccional de Habeas Data, determinando así que es de obligatorio acatamiento y que en caso de “desconocimiento de estas interpretaciones, se estará a lo dispuesto en la Constitución de la República del Ecuador, la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional y el Reglamento de Sustanciación de Procesos de la Competencia de la Corte Constitucional” (Corte Constitucional del Ecuador, 2015).

2.4.7.3. Sentencia No. 55-14-JD/20. CASO No. 55-14-JD Revisión de garantías (JD) Hábeas data y rectificación de datos personales.

Esta sentencia de revisión es particular porque constituye jurisprudencia vinculante, respecto a la acción de habeas data.

El motivo radicaba en la negativa de rectificar datos en el Sistema Integral Informático de la Policía Nacional (SIIPNE) y su decisión fue la siguiente:

La Corte admitió que se presente la acción cuando se haya configurado la negativa tácita de la solicitud por la falta de contestación oportuna. Además, se alejó expresamente de la regla jurisprudencial establecida en la sentencia 182-15-SEP-CC, y puntualizó que no se requiere comprobar la vulneración de otro derecho constitucional u otro perjuicio, ya que la acción procede ante la sola existencia de datos imprecisos, el mero uso indebido de información personal, contra la voluntad del titular o sin autorización judicial o legal. Finalmente, dispuso la rectificación de la información, que el Ministerio de Gobierno regule el funcionamiento del SIIPNE y que el Consejo de la Judicatura difunda la sentencia. (Corte Constitucional del Ecuador, 2020)

CAPITULO III

MARCO METODOLÓGICO

3.1. Tipo y diseño de la investigación.

La investigación es de tipo transversal, no experimental, aplicada ya que se pretende contribuir, desde los resultados obtenidos con una propuesta que permita dar una solución a la problemática planteada.

3.1.1. *Diseño*

La investigación está diseñada como investigación de campo y bibliográfico, describe la problemática de manera directa a través de las técnicas, observación, entrevista y encuesta aplicadas, a concluir la problemática suscitada en función de un enfoque práctico. Por medio del acercamiento a la fuente se pudo obtener valiosa información a través de un proceso técnico-científico. (Hernandez, Sampieri, & Baptista, 2019)

3.1.1.1. Investigación de campo

Según Arias (2014), la investigación de campo es aquella que vive en la recolección de datos directamente de los sujetos indagados, o de la del entorno donde suceden los hechos (datos primarios), sin manipular o controlar variable alguna, es decir, el investigador obtiene la información, pero no altera las condiciones existentes.

Dentro de la investigación de campo, se aplicarán instrumentos de investigación para conocer de cerca la percepción de la ciudadanía y de los profesionales del derecho, a fin de conocer su opinión y percepción sobre el tema a investigar, los derechos constitucionales que se encuentran reconocidos, así como los mecanismos legales que están vigentes en la legislación ecuatoriana.

3.1.1.2. Investigación bibliográfica

La investigación bibliográfica se caracteriza por la utilización de los datos secundarios como fuente de información. Utilizar varias fuentes distintas, cotejándolas cuidadosamente. En síntesis, la investigación bibliográfica consiste en la búsqueda, recopilación, organización, valoración, crítica e información de datos bibliográficos. (UNAM, 2018)

En la presente investigación se utilizó fuentes secundarias como revisas, artículos científicos indexados y periódicos en internet, o aquellos documentos que permitan recopilar

evidencia sobre lo que acontece a las TIC y como estas pueden afectar los derechos humanos y constitucionales de las personas.

3.2. Enfoque.

El enfoque de la investigación hace referencia a un enfoque mixto, cualitativo cuantitativo. La metodología que se utilizará en esta investigación tendrá un enfoque predominante cualitativo por que analizará la realidad que ha generado la irrupción de la tecnología en lo que respecta a los derechos de los ciudadanos, a la vez que es indispensable el análisis de la teoría que se encuentra en constante creación; y cuantitativo por que se obtendrán datos numéricos que serán tabulados estadísticamente desde la aplicación de los instrumentos o herramientas de recolección de datos, con el fin de medir la opinión y análisis de la ciudadanía.

3.2.1. Cualitativa

La investigación cualitativa es el procedimiento metodológico que utiliza palabras, textos, discursos, dibujos, gráficos e imágenes para construir un conocimiento de la realidad social, en un proceso de conquista-construcción-comprobación teórica desde una perspectiva holística. La perspectiva cualitativa de la investigación intenta acercarse a la realidad social a partir de la utilización de datos no cuantitativos. (Álvarez, Camacho, & Maldonado, 2020)

Se utilizará el enfoque cualitativo porque se hará una descripción de lo recopilado en el entorno de los profesionales del derecho, que permita establecer un punto de reflexión sobre lo que ocurre actualmente con la problemática de estudio en la presente investigación.

3.2.2. Cuantitativa

La investigación cuantitativa es aquella en la que se recogen y analizan datos cuantitativos sobre variables. La investigación cualitativa evita la cuantificación. Los investigadores cualitativos hacen registros narrativos de los fenómenos que son estudiados mediante técnicas como la observación participante y las entrevistas no estructuradas.

La investigación cuantitativa trata de determinar la fuerza de asociación o correlación entre variables, la generalización y objetivación de los resultados a través de una muestra para hacer inferencia a una población de la cual toda muestra procede. Tras el estudio de la asociación o correlación pretende, a su vez, hacer ilación causal que explique por qué las cosas suceden o no de una forma determinada. (Fisterra, 2020)

3.2.3. Descriptivo

Los estudios descriptivos se sitúan sobre una base de conocimientos más sólida que los exploratorios. El problema muchas veces es de naturaleza práctica, y su solución transita por el conocimiento de las causas, pero las hipótesis causales sólo pueden partir de la descripción completa y profunda del problema en cuestión. (Jimenez, 1998)

Porque la investigación detalla el problema en sus causas y consecuencias, desde la asociación de variables, por cuanto en la investigación se establece la relación entre la variable independiente y la variable dependiente.

3.3. Población y muestra.

3.3.1. Características de la población

La población está compuesta de los profesionales del derecho en libre ejercicio profesional, en la ciudad de Guayaquil.

3.3.2. Delimitación de la población

La población para el presente estudio se integra de la siguiente manera:

Tabla 2. Población

DETALLE	CANTIDAD
Ciudadanos en Guayaquil	<u>2'257.819</u>
Total	<u>2'257.819</u>

Tabla 3 Delimitación de la población.

Fuente: Ecuador en cifras (2021).

3.3.3. Tipo de muestra

La muestra debe lograr una representación adecuada de la población, en la que se reproduzca de la mejor manera los rasgos esenciales de dicha población que son importantes para la investigación. (USON, 2018)

La selección de la muestra será de representación cuantitativa con muestreo probabilístico, que tiene por objeto afirmar que los instrumentos de interés estén en los parámetros representados apropiadamente. Debido a que el objeto de estudio, en este caso, se centra en un aspecto de derechos específico, se someterán a la aplicación del cuestionario, a la mayor viabilidad posible.

3.3.4. *Tamaño de la Muestra*

Determinar el tamaño de la muestra que se va a seleccionar es un paso importante en cualquier estudio de investigación de mercados, se debe justificar convenientemente de acuerdo al planteamiento del problema, la población, los objetivos y el propósito de la investigación. (Psyma, 2015)

Para este tipo de estudio se procede a utilizar el muestreo probabilístico al azar, para obtener una muestra representativa de los sujetos de estudio, se procedió a aplicar la siguiente formula de muestreo probabilístico aleatorio simple:

Aplicación de la fórmula:

$$n = \frac{N \times Z^2 \times p \times q}{d^2 (N - 1) + Z^2 \times p \times q}$$

En donde:

N = tamaño de la población

Z = nivel de confianza

P = probabilidad de éxito, o proporción esperada

Q = probabilidad de fracaso

D = precisión (Error máximo admisible en términos de proporción).

$$n = \frac{2'257.819 \times 1,96^2 \times 0,5 \times 0,5}{0,05^2 (2'257.819 - 1) + 1,96^2 \times 0,5 \times 0,5}$$

$$n = \mathbf{384}$$

Por tanto, la muestra estará conformada por 384 ciudadanos en la ciudad de Guayaquil.

3.4. Proceso de selección de la muestra.

Para el proceso de selección de la muestra, se utilizó el muestreo aleatorio. Una vez calculado el tamaño muestral apropiado, se tiende a asegurar que la muestra represente adecuadamente a la población en función de unas variables seleccionadas. Se obtienen

estimaciones más precisas y su objetivo es conseguir una muestra lo más semejante posible a la población en lo que a las variables estratificadas se refiere. (USON, 2018)

3.5. Los métodos y las técnicas.

3.5.1. Métodos Teóricos

Para el cumplimiento de las tareas se realizarán los siguientes métodos de investigación:

3.5.2. Método Analítico Sintético

El método sintético se refiere a la síntesis de las cosas o de los fenómenos; la palabra síntesis, del griego *synthesis* significa composición de un todo mediante la unión de sus partes, definiendo que relación tienen entre sí y de qué manera afectan la realización del fenómeno en cuestión, así, hasta completar nuevamente el todo. (Raul, 2009)

Este método lleva, por ende, de las causas a los efectos y de los principios a las conclusiones. Porque maneja juicios considerando cada una de las causas, las cuales son clasificadas, para conocer su principal origen y llegar a una conclusión.

3.5.3. Método analítico

El método analítico de investigación es una forma de estudio que implica habilidades como el pensamiento crítico y la evaluación de hechos e información relativa a la investigación que se está llevando a cabo. La idea es encontrar los elementos principales detrás del tema que se está analizando para comprenderlo en profundidad. (Rodríguez, 2020)

Para estudiar las diferentes causas particulares a una causa generalizada y de general a particular, se aplica una lógica en entender y explicar las causas del proceso.

3.6. Técnicas o instrumentos.

Las técnicas aplicadas en la investigación y que permitieron la recolección de datos son la encuesta a la ciudadanía; a partir de la recolección de datos reales se realizaron la tabulación para representar en cuadros estadísticos los resultados obtenidos, donde se evidenciaron en diagrama de pastel el porcentaje y del análisis de los resultados de las preguntas planteadas permitirá dar soluciones posibles a la problemática abordada. (Hernandez, Sampieri, & Baptista, 2019)

3.6.1. Encuesta

Orientada a la recolección de datos proporcionados por los ciudadanos de la ciudad de Guayaquil. El instrumento de medición utilizado será un cuestionario de preguntas cerradas,

donde los encuestados deberán responder sobre los parámetros considerados como factores críticos en la decisión del uso de sus datos por las diferentes plataformas tecnológicas.

3.6.2. Entrevista a Expertos

La entrevista fue dirigida a cuatro profesionales del Derecho Constitucional y Derechos Humanos en el cantón Guayaquil, Provincia del Guayas, quienes validaron la problemática planteada, así como el objetivo general y los específicos.

3.7. Criterios de inclusión.

La encuesta será aplicada a personas entre un rango de edad desde dieciséis (16) años hasta setenta y cuatro (74) años, de ambos sexos, que vivan en la ciudad de Guayaquil.

3.8. Gestión de los datos.

Para la recolección de datos del proyecto de investigación se implementarán técnicas como el uso de las redes sociales para poder realizar las encuestas de manera física y digital. La tabulación de los datos se los realizará a través de los registros de Google Drive y se los exportará a un libro en Excel para la presentación de los resultados por medio de la tabulación en tablas y gráficos de pastel.

3.9. Hipótesis del estudio.

La hipótesis del presente estudio es:

H1: El uso de las TICs, vulneran los derechos de los ciudadanos ecuatorianos, por la deficiente legislación que regule el tratamiento de datos.

Variable	Definición
TIC	Las tecnologías de la información y comunicación, conocidas por su abreviatura como TIC, son un conjunto de tecnologías requeridas para el almacenamiento, recuperación, proceso y comunicación de la información. ... Inmaterialidad, su materia prima es la información en múltiples códigos y formas. (Heinze, 2017)
Vulneración de derechos	El concepto de “vulneración de derechos” corresponde a cualquier trasgresión a los derechos, por lo que los Estados deben realizar todas

	las acciones destinadas a prevenir estos hechos y a entregar mecanismos de restitución de derechos una vez ya vulnerados. (Observatorio de derechos, 2021)
Legislación	La legislación es un conjunto de normas y leyes que regulan las relaciones entre las personas de un país o de un sector determinado. (Trujillo, 2020)
Tratamiento de datos	El tratamiento de los datos se refiere a cualquier operación o conjunto de operaciones efectuadas sobre datos particulares o conjunto de datos particulares, mediante procedimientos manuales o automatizados relacionadas con la obtención, uso, registro, distribución, conformación, utilización, comunicación, transmisión, almacenamiento, posesión o destrucción o habilidad de datos personales. (Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales, 2020)

Tabla 4. Definición conceptual de variables.

Elaborado: Omar Altamirano Villena. (2021)

A partir de la definición conceptual de las variables independiente y dependiente se construirá el instrumento de recolección de datos.

3.10. Variables operativas, indicadores y parámetros aplicados.

3.10.1. Operacionalización de variables.

VARIABLES INDEPENDIENTE DE LA HIPOTESIS	SUBVARIABLE	DIMENSIONES	TIPO DE PREGUNTA	PREGUNTA AL ENCUESTADO	OPCIONES DE RESPUESTAS
TICs	Tecnología	Teléfono inteligente; computadoras, Tv inteligentes; Internet; cámaras de seguridad	Escala de Likert Pregunta Cerrada	¿Usted cree que con el acceso a las Tecnologías de la Información y Comunicación (TICs) se podrían ver	Totalmente de acuerdo Medianamente de acuerdo Estoy de Acuerdo Medianamente en desacuerdo

				perjudicados o vulnerados sus derechos?	Totalmente en desacuerdo No tengo conocimiento
TICs	Tecnología	Teléfono inteligente; computadoras, Tv inteligentes; Internet; cámaras de seguridad	Selección múltiple	¿Con que Tecnología de Información y Comunicación (TICs) usted cree que se podrían vulnerar los derechos antes señalados?	Radio Internet Teléfono convencional Televisor Celular básico llamadas y msm Celular inteligente (Smartphone) Internet Computadoras Ninguna de las anteriores No tengo conocimiento
	Tecnología	Teléfono inteligente; computadoras, Tv inteligentes; Internet; cámaras de seguridad	Escala de Likert	¿Usted cree que el sistema de cámaras de vigilancia instalado por el Ecu911, puede limitar o vulnerar derechos?	Totalmente de acuerdo Medianamente de acuerdo Estoy de Acuerdo Medianamente en desacuerdo Totalmente en desacuerdo No tengo conocimiento
Plataformas tecnológicas	Tecnología	Redes Sociales, Aplicaciones;	Selección múltiple	¿ Con que redes sociales usted cree que se	Facebook WhatsApp YouTube

	Software; Inteligencia Artificial	podrían vulnerar los derechos antes señalados?	Snapchat Instagram Tik Tok LinkedIn Telegram Facebook Messenger Spotify Ninguna de las anteriores No tengo conocimiento
--	---	--	---

Vulneración de derechos	Derechos	D. a la protección de datos de carácter personal D. a la inviolabilidad y al secreto de correspondencia física y virtual D. a la libertad de expresión D. a la libertad de información D. a la intimidad personal y familiar D. al honor y buen nombre D. a la imagen D. a la protesta D. a la libertad de	Pregunta de selección múltiple	Si la respuesta fue afirmativa en la pregunta anterior. ¿Cuáles derechos cree usted que se verían perjudicados o vulnerados por el uso de las TICs?	D. a la protección de datos de carácter personal D. a la inviolabilidad y al secreto de correspondencia física y virtual D. a la libertad de expresión D. a la libertad de información D. a la intimidad personal y familiar D. al honor y buen nombre D. a la imagen D. a la protesta D. a la libertad de
--------------------------------	----------	--	--------------------------------	---	--

	tránsito y libre movilidad D. Ninguna de las anteriores No tengo conocimiento			tránsito y libre movilidad D. Ninguna de las anteriores No tengo conocimiento
Derechos	Derechos Humanos y Fundamentales	Escala de Likert	¿Usted cree que con el uso de las redes sociales se podrían ver perjudicados o vulnerados sus derechos?	Totalmente de acuerdo Medianamente de acuerdo Estoy de Acuerdo Medianamente en desacuerdo Totalmente en desacuerdo No tengo conocimiento
Derechos	D. a la protección de datos de carácter personal D. a la inviolabilidad y al secreto de correspondenci a física y virtual D. a la libertad de expresión D. a la libertad de información D. a la intimidad	Pregunta de selección múltiple	Si respondió si en la pregunta anterior. ¿Cuáles derechos cree usted que se restringirían o vulnerarían?	D. a la protección de datos de carácter personal D. a la inviolabilidad y al secreto de correspondenci a física y virtual D. a la libertad de expresión D. a la libertad de información D. a la intimidad

	personal y familiar D. al honor y buen nombre D. a la imagen D. a la protesta D. a la libertad de tránsito y libre movilidad D. Ninguna de las anteriores No tengo conocimiento			personal y familiar D. al honor y buen nombre D. a la imagen D. a la protesta D. a la libertad de tránsito y libre movilidad D. Ninguna de las anteriores No tengo conocimiento
Derechos		Escala de Likert	¿Usted cree que las empresas y/o el Estado, al recopilar datos o información de personas en la web, dispositivos electrónicos y de vigilancia, vulneran o vulnerarían derechos de los ciudadanos?	Totalmente de acuerdo Medianamente de acuerdo Estoy de Acuerdo Medianamente en desacuerdo Totalmente en desacuerdo No tengo conocimiento
Derechos	D. a la protección de datos de carácter personal D. a la inviolabilidad	Pregunta de selección múltiple	Si respondió si en la pregunta anterior. ¿Cuáles derechos de los ciudadanos cree usted que se restringirían o	D. a la protección de datos de carácter personal D. a la inviolabilidad

	<p>y al secreto de correspondencia física y virtual D. a la libertad de expresión D. a la libertad de información D. a la intimidad personal y familiar D. al honor y buen nombre D. a la imagen D. a la protesta D. a la libertad de tránsito y libre movilidad D. Ninguna de las anteriores No tengo conocimiento</p>	vulnerarían?	<p>y al secreto de correspondencia física y virtual D. a la libertad de expresión D. a la libertad de información D. a la intimidad personal y familiar D. al honor y buen nombre D. a la imagen D. a la protesta D. a la libertad de tránsito y libre movilidad D. Ninguna de las anteriores No tengo conocimiento</p>
Derechos	Escala de Likert	¿Usted cree que las empresas que se dedican a recopilar datos o información personal, al venderlas vulneran derechos de los ciudadanos?	<p>Totalmente de acuerdo Medianamente de acuerdo Estoy de Acuerdo Medianamente en desacuerdo Totalmente en desacuerdo No tengo conocimiento</p>

Derechos	D. a la protección de datos de carácter personal D. a la inviolabilidad y al secreto de correspondencia física y virtual D. a la libertad de expresión D. a la libertad de información D. a la intimidad personal y familiar D. al honor y buen nombre D. a la imagen D. a la protesta D. a la libertad de tránsito y libre movilidad D. Ninguna de las anteriores No tengo conocimiento	Pregunta de selección múltiple	Si respondió si en la pregunta anterior. ¿Cuáles derechos de los ciudadanos cree usted que se restringirían o vulnerarían?	D. a la protección de datos de carácter personal D. a la inviolabilidad y al secreto de correspondencia física y virtual D. a la libertad de expresión D. a la libertad de información D. a la intimidad personal y familiar D. al honor y buen nombre D. a la imagen D. a la protesta D. a la libertad de tránsito y libre movilidad D. Ninguna de las anteriores No tengo conocimiento
Derechos	Derechos Humanos y Fundamentales	Escala de Likert	¿Usted considera que, con el avance de la tecnología, deberíamos tener	Totalmente de acuerdo Medianamente de acuerdo Estoy de

			derecho a decidir qué uso se da a nuestra información personal?	Acuerdo Medianamente en desacuerdo Totalmente en desacuerdo No tengo conocimiento
Derechos	Derechos Humanos y Fundamentales	Escala de Likert	¿Usted cree que debería de existir un derecho en el que toda la información que usted haya generado o compartido sea eliminada de las bases de datos, tanto privadas como gubernamentales ?	Totalmente de acuerdo Medianamente de acuerdo Estoy de Acuerdo Medianamente en desacuerdo Totalmente en desacuerdo No tengo conocimiento
Derechos	Derechos Humanos y Fundamentales	Escala de Likert	¿Usted considera que, con el avance de la tecnología, deberíamos tener derecho a decidir qué uso se da a nuestros datos o información personal?	Totalmente de acuerdo Medianamente de acuerdo Estoy de Acuerdo Medianamente en desacuerdo Totalmente en desacuerdo No tengo conocimiento

Derechos	Derechos Humanos y Fundamentales	Net Promotor Score (NPS)	En una escala del 1 al 10 siendo el 1 lo más bajo y 10 lo más alto, ¿qué tan capacitadas cree que se encuentran las instituciones públicas del Ecuador para evitar el robo de datos y reaccionar exitosamente para solucionar el problema y proteger la información de sus ciudadanos?	1 2 3 4 5 6 7 8 9 10
Derechos	Derechos Humanos y Fundamentales	Dicotómica		No tengo conocimiento
Derechos	Derechos Humanos y Fundamentales	Escala de Likert	¿Cree usted que la Asamblea Nacional del Ecuador debe de preocuparse por legislar en el área tecnológica que involucre al ser humano, entre ello, el tratamiento de datos personales y seguridad de información	Totalmente de acuerdo Medianamente de acuerdo Estoy de Acuerdo Medianamente en desacuerdo Totalmente en desacuerdo No tengo conocimiento

Tabla 5. Operacionalización de variables – Encuestas.

Fuente: Investigación de campo. (2021)

Elaborado por: Omar Altamirano Villena. (2021)

VARIABLES INDEPENDIENTE DE LA HIPOTESIS	SUBVARIABLE	DIMENSIONES	PREGUNTA AL ENCUESTADO	TIPO DE RESPUESTA
	TICs	Tecnología	¿Cómo cree usted que las (TICs), Redes Sociales y aplicaciones tecnológicas, ¿causan	Abierta
	Plataformas tecnológicas	Tecnología	o causarían violación de derechos a los usuarios? ¿Cuál sería el proceso para esto?	
	Plataformas tecnológicas	Tecnología	¿Qué opinión le merece, el uso que las empresas desarrolladoras de tecnología y el Estado dan a los datos o información obtenida de los usuarios, mediante cualquier plataforma tecnológica?	Abierta
VARIABLES DEPENDIENTE DE LA HIPOTESIS	Vulneración de derechos	Derechos Humanos	¿Cómo experto, que situaciones pueden realizarse con la información o datos recopilados por el sistema de cámaras	Abierta
VARIABLES INDEPENDIENTE DE LA HIPOTESIS	Plataformas tecnológicas	Tecnología	de seguridad instalada en áreas públicas por el Estado? ¿Esto, podría afectar de alguna manera a los	

		derechos de los ciudadanos?	
Plataformas tecnológicas	Tecnología	¿Cree que la práctica de recolección de datos mediante cookies o métodos de captación de información adicional es indiscriminada, al recopilar datos sin conocimiento ni consentimiento del usuario? ¿Qué puede provocar?	Abierta
Plataformas tecnológicas	Tecnología	Para el usuario, ¿Qué consecuencias traería la recolección de sus datos por parte de empresas y entidades gubernamentales? ¿Conoce el proceso?	Abierta
Plataformas tecnológicas	Tecnología	¿Tiene conocimiento si la recolección de información de datos digitales está normada legalmente por el Estado Ecuatoriano?	Abierta
Plataformas tecnológicas	Tecnología	¿Cree usted que el Estado Ecuatoriano debería de normar el uso, captación y venta de datos de usuarios por parte de la Empresas	Abierta

			desarrolladoras tecnológicas y de las entidades gubernamentales?	
VARIABLES DEPENDIENTE DE LA HIPOTESIS	Vulneración de derechos	Derechos Humanos	En su opinión, ¿Cuál sería, la forma óptima y segura de utilizar las TIC, Redes Sociales y Aplicaciones tecnológicas? para evitar la captación de nuestra información y no ser víctimas de vulneración de derechos?	Abierta
VARIABLES INDEPENDIENTE DE LA HIPOTESIS	TICs	Tecnología		
	Plataformas tecnológicas	Tecnología		
VARIABLES	SUBVARIABLE	DIMENSIONES	TIPO DE PREGUNTA	
VARIABLES DEPENDIENTE DE LA HIPOTESIS	Vulneración de derechos	Derechos Humanos	En base al derecho contemplado en el numeral 2 del Art. 16 de la Constitución del Ecuador que determina: "Todos los seres humanos, en forma individual o colectiva, tienen derecho a: El acceso universal a las tecnologías de información y comunicación". ¿Cree usted que su ejercicio tendría como efecto la vulneración de otros derechos de los ciudadanos, contemplados en la Constitución y Tratados Internacionales de	Abierta

Derechos Humanos?
¿Cuáles? y ¿Por qué?

Vulneración de derechos	Derechos Humanos	Cuál es su opinión sobre el uso que se podría dar a los datos que recolectan las Empresas y el Estado. ¿Tiene alguna consecuencia negativa en relación a los derechos de los ciudadanos?	Abierta
----------------------------	---------------------	---	---------

Vulneración de derechos	Derechos Humanos	Cómo usuario de internet y redes sociales, cree que la información o datos personales proporcionada por usted, ¿serviría para que se configure la violación de sus derechos? ¿Cuáles derechos sería y por qué?	Abierta
Vulneración de derechos	Derechos Humanos	¿Considera que el desarrollo de las TICs, software y programas como la inteligencia artificial podrían vulnerar derechos? ¿Cuáles y por qué?	Abierta

Tabla 6. Operacionalización de variables – Entrevistas.

Fuente: Investigación de campo (2021).

Elaborado por: Omar Altamirano Villena. (2021)

CAPITULO IV

ANÁLISIS DE LOS RESULTADOS

4.1. Conclusiones Parciales.

4.1.1. Encuesta de uso de TIC

4.1.1.1. Rango de uso de TICs a nivel nacional.

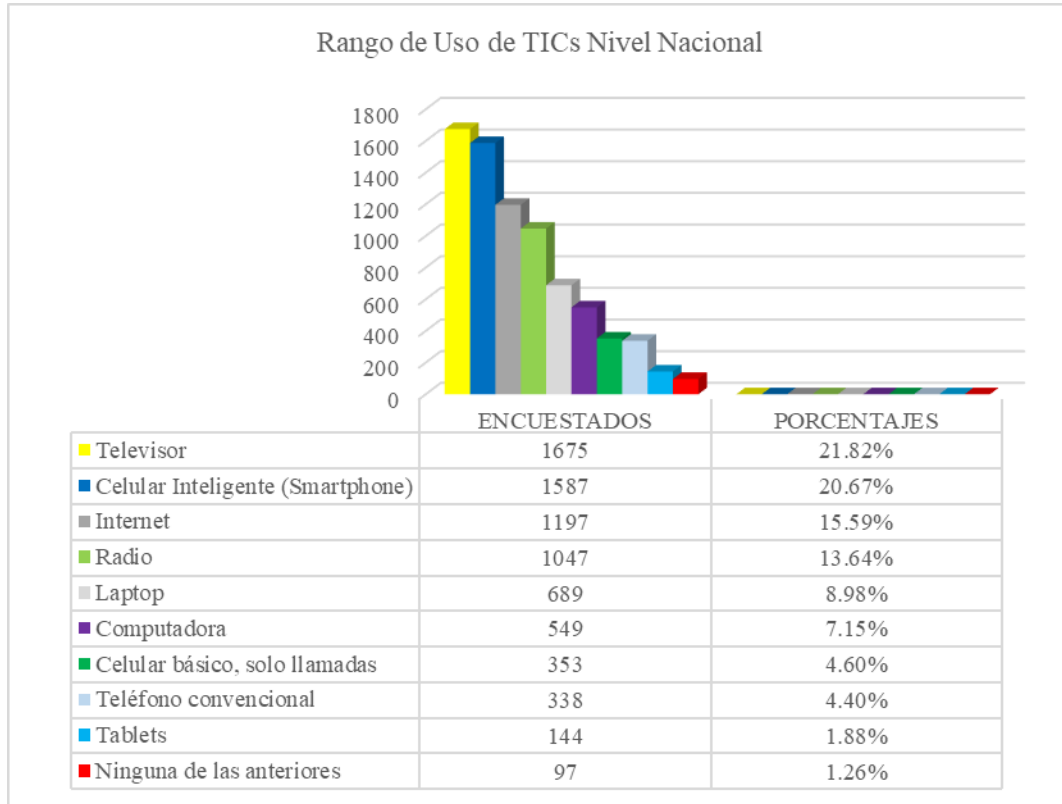


Gráfico 1. Rango de uso de TICs a nivel nacional.

Fuente: Investigación de campo (2021).

Elaborado por: Omar Altamirano Villena (2021)

Nota: Datos Obtenido del Análisis de las TICs, Redes Sociales, Big Data e Inteligencia Artificial, como herramientas tecnológicas para su aplicación en campañas electorales en los Gobiernos Seccionales del Ecuador. Autor: Omar Altamirano Villena (2021).

Los datos presentados en la gráfica presentan la opinión de siete mil seiscientos setenta y seis (7.676) ciudadanos ecuatorianos mayores de dieciocho (18) años, quienes opinaron sobre sus preferencias de uso de TIC. En el gráfico de barras se observan varias fuentes, pero para esta investigación se analizaron las preferencias del internet, celular inteligente, laptop, tablet y computadora.

Del total de la población se puede observar que las TICs con mayor porcentaje de uso es el celular inteligente o smartphone con 20,67% (1.587 ciudadanos), luego se encuentra el internet con 15,59% (1.197 ciudadanos), en tercer lugar, tenemos a el 8,98%, (689 ciudadanos) luego tenemos a la computadora con 7,15% de uso (549 ciudadanos) y por último la tablet con 1,88% (144 ciudadanos). Cabe recalcar que el INEC (Instituto Nacional de Estadísticas y Censo) agrupa a la computadora, laptop y tablet dentro de la categoría ordenadores donde el porcentaje de preferencia de uso agrupando en una sola categoría los tres dispositivos sería de 18,01% (1.382 ciudadanos).

Desde el punto de vista legal, el uso de las tecnologías se encuentra amparada en la Ley Orgánica de Telecomunicaciones y Ley de Comercio Electrónico, las mismas regula los servicios de difusión, así como los negocios jurídicos de los usuarios, entre otros respectivamente.

4.1.1.2. Uso de TICs en el cantón Guayaquil Prov. del Guayas.

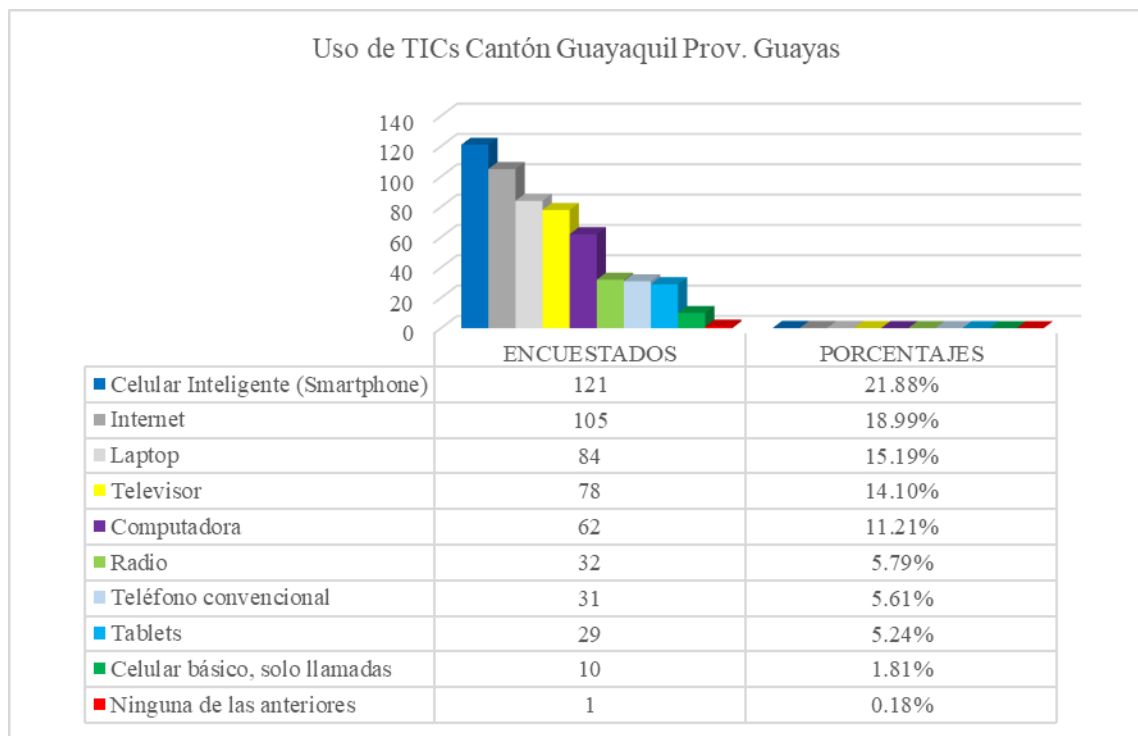


Gráfico 2. Uso de TICs en el cantón Guayaquil Prov. del Guayas.

Fuente: Investigación de campo (2021).

Elaborado por: Omar Altamirano Villena (2021)

Nota: Datos Obtenido de la Tesis Análisis de las TICs, Redes Sociales, Big Data e Inteligencia Artificial, como herramientas tecnológicas para su aplicación en campañas electorales en los Gobiernos Seccionales del Ecuador. Autor: Omar Altamirano Villena.

En esta encuesta se obtuvo que del total de quinientos cincuenta y tres (553) ciudadanos encuestados del cantón Guayaquil, mencionan que las TICs con mayor porcentaje de preferencia de uso fue el celular inteligente o smartphone con 21,88% (121 ciudadano), internet con 18,99% (105 ciudadanos), laptop con 15,19% (84 ciudadanos), la computadora con 11,21% (62 ciudadanos) y la tablet con 5,24% de preferencia de uso (29 ciudadanos). El porcentaje de preferencia de uso agrupando en una sola categoría los tres dispositivos seria de 31,64% (175 ciudadanos).

4.1.2. Exposición y análisis de los resultados recabados mediante encuestas realizada a los ciudadanos del cantón Guayaquil.

1. Características etarias

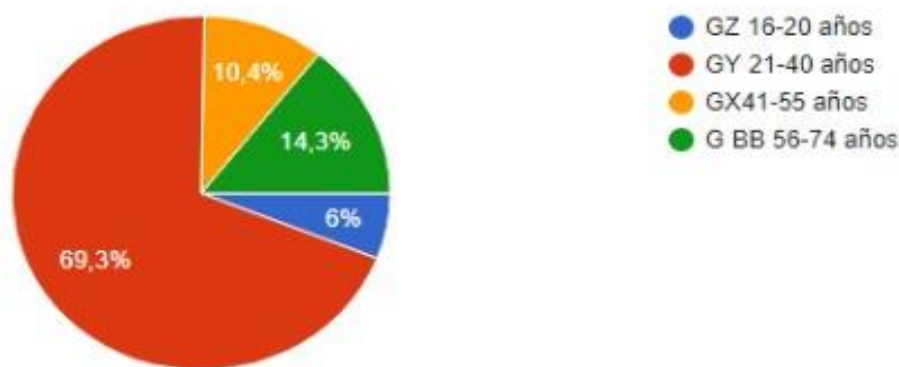


Gráfico 3. Características etarias.

Fuente: Investigación de campo (2021).

Elaborado por: Omar Altamirano Villena (2021)

Análisis:

La muestra objeto de la encuesta estuvo conformada por un 69.3% de personas comprendidas entre veintiuno (21) y cuarenta (40) años, seguido de un 14.3% de personas mayores a cincuenta y seis (56) años. En una minoría se encontraron los ciudadanos entre

cuarenta y un (41) y cincuenta y cinco (55) años que representaron un 10.4% y un 6% correspondió a jóvenes entre dieciséis (16) y veinte (20) años.

2. Sexo

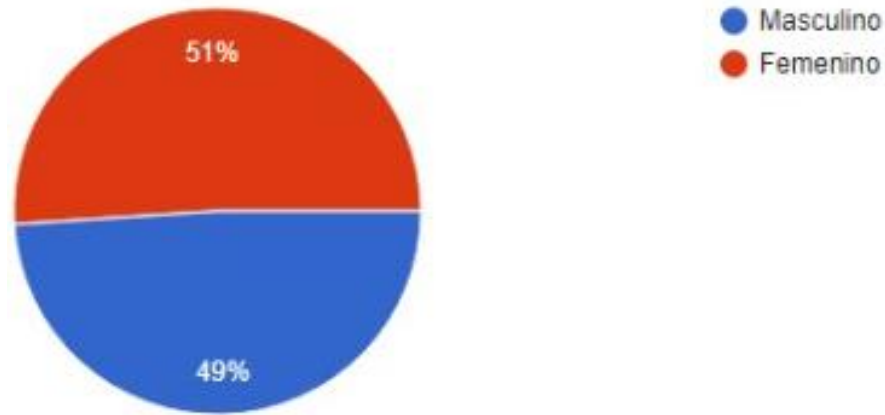


Gráfico 4. Sexo.

Fuente: Investigación de campo (2021).

Elaborado por: Altamirano (2021)

Análisis:

En cuanto a la identificación de género, un 51% de los ciudadanos encuestados se determinaron como de sexo femenino, mientras que un 49% se determinó como de sexo masculino.

3. Instrucción Educativa

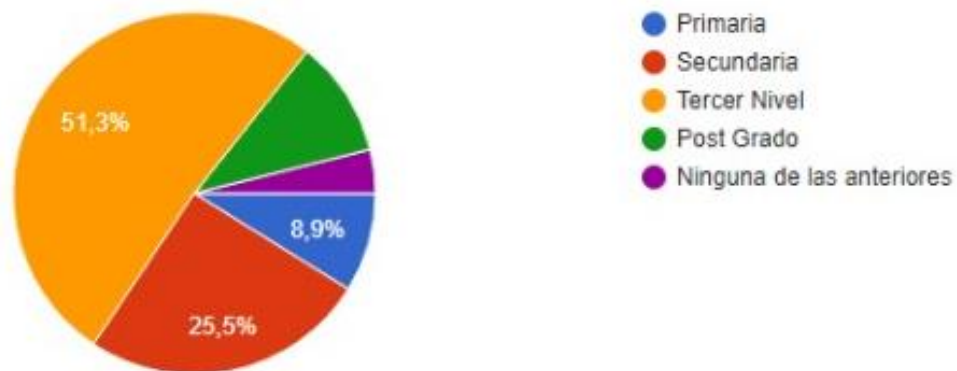


Gráfico 5. Instrucción Educativa.

Fuente: Investigación de campo (2021)

Elaborado por: Omar Altamirano Villena (2021)

Análisis:

De los ciudadanos encuestados el 51% de ellos tienen una formación educativa de tercer nivel, seguido de un 25.5% que tienen instrucción secundaria, un 10% con nivel de postgrado y un 8.9% con la instrucción de primaria.

4. ¿Cree que con el acceso a las TIC se podrían ver perjudicados o vulnerados sus derechos?

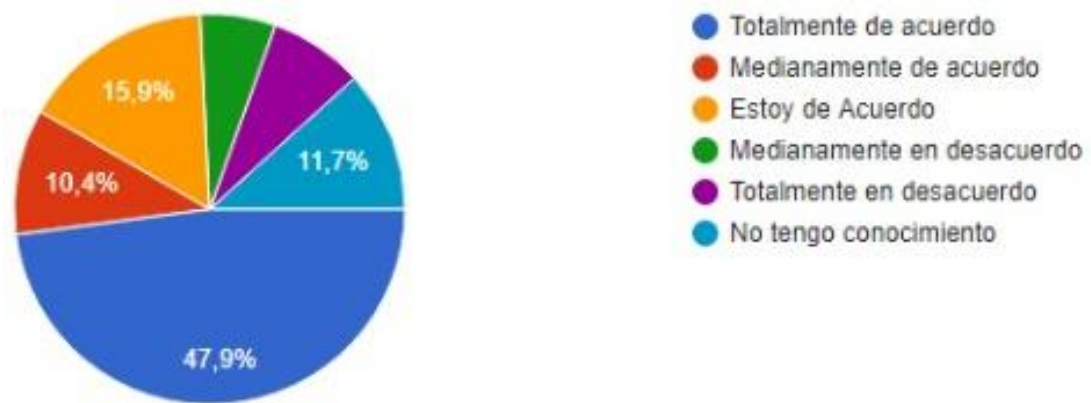


Gráfico 6. Opinión sobre acceso a TIC y vulneración de derechos.

Fuente: Investigación de campo (2021).

Elaborado por: Omar Altamirano Villena (2021)

Análisis:

De los ciudadanos encuestados el 47.9% de ellos opina que las TIC son un mecanismo por donde se podría ver perjudicados o vulnerados sus derechos. Un 15,9% indica estar de acuerdo con esta afirmación, mientras que un 11.7% mencionaron que no tienen conocimiento sobre esta situación.

5. ¿Cuáles derechos se verían perjudicados o vulnerados por el uso de las TICs?

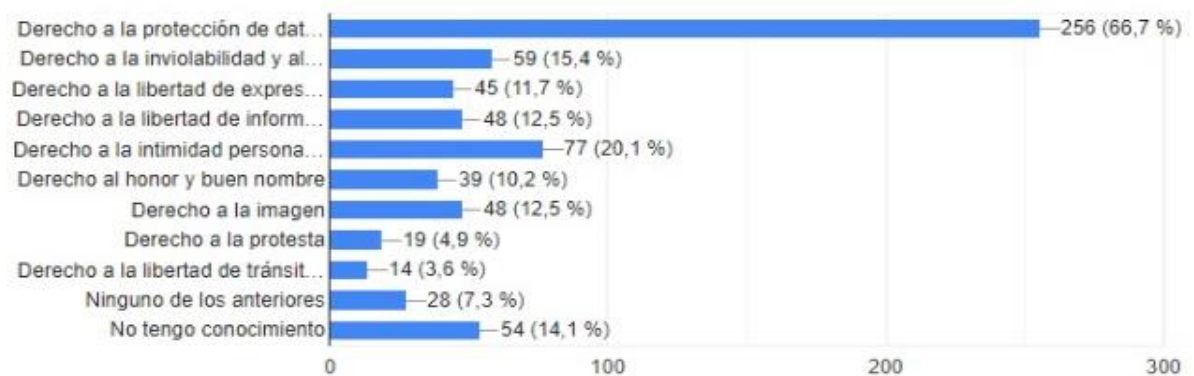


Gráfico 7. Derechos que se ven perjudicados por acceso a TICs.

Fuente: Investigación de campo (2021).

Elaborado por: Omar Altamirano Villena (2021).

Análisis:

En cuanto a cuáles derechos cree el ciudadano que se verían perjudicados o vulnerados por el uso de las TIC, un 66.7% de los ciudadanos encuestados afirmaron que sienten que sus derechos a la protección de datos privados se ven vulnerados, mientras que un 20.1% afirma que no se respeta el derecho a la intimidad personal.

6. ¿Con que TIC cree que se podrían vulnerar los derechos?

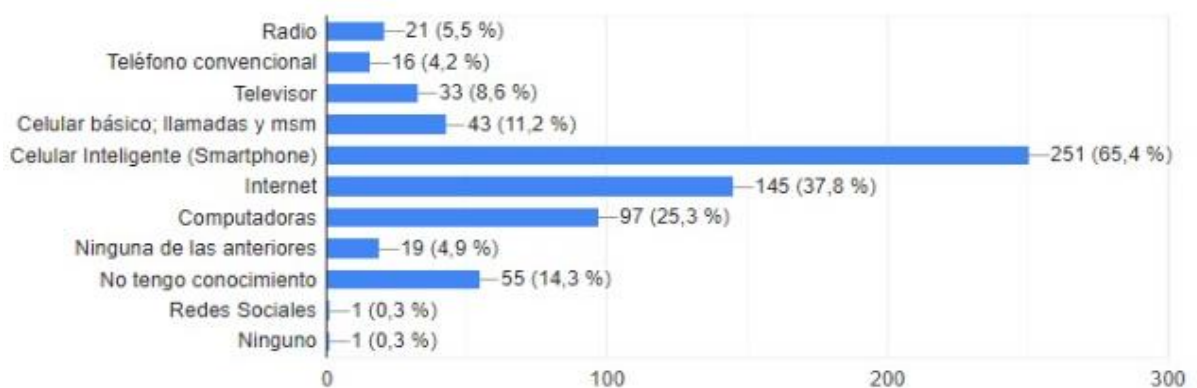


Gráfico 8. Medio por el que TIC puede vulnerar sus derechos.

Fuente: Investigación de campo (2021).

Elaborado por: Omar Altamirano Villena (2021)

Análisis:

En cuanto a los medios usados por las Tecnología de Información y Comunicación (TICs) cree que se podrían vulnerar sus derechos, un 65.4% de los ciudadanos encuestados afirmaron que los smartphones son el medio más frecuente que se utiliza, mientras que un 37.8% indica que el internet es otro mecanismo que usa TIC para acceder a la información, un 25.3% también percibe que la computadora es otro de los mecanismos de TIC desde los cuales pueden verse vulnerados sus derechos.

7. ¿Con el uso de las redes sociales se podrían ver perjudicados o vulnerados sus derechos?

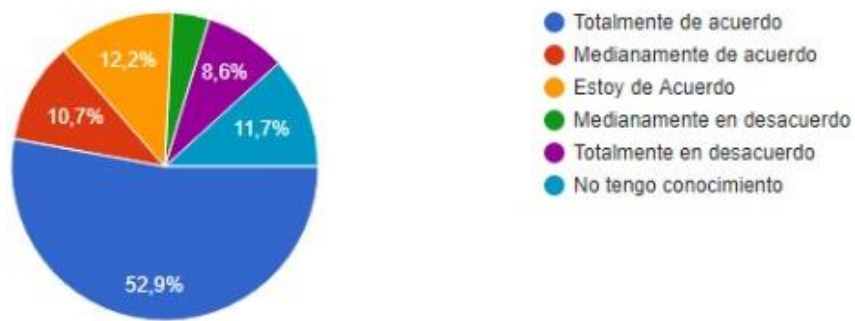


Gráfico 9. Opinión sobre uso de Redes sociales y vulneración de derechos.

Fuente: Investigación de campo (2021).

Elaborado por: Omar Altamirano Villena (2021)

Análisis:

En cuanto al uso de las redes sociales donde se podrían ver perjudicados o vulnerados sus derechos, un 52.9% de los ciudadanos encuestados afirmaron estar totalmente de acuerdo con esta afirmación, un 12.2% indica que están de acuerdo, un 11.7% dijeron que no tienen conocimiento, mientras que un 10.7% dijeron estar medianamente de acuerdo, un 8.6% están totalmente en desacuerdo.

8. ¿ Con que redes sociales cree que se podrían vulnerar los derechos?

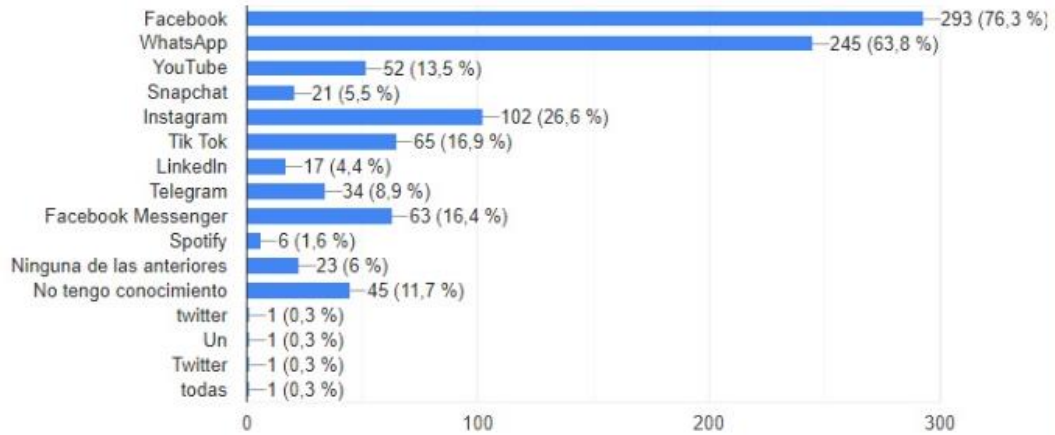


Gráfico 10. Redes sociales por las que puede vulnerar sus derechos.

Fuente: Investigación de campo (2021).

Elaborado por: Omar Altamirano Villena (2021)

Análisis:

En cuanto a con que redes sociales cree que se podrían vulnerar sus derechos, un total de 76.3% eligió a Facebook, un 63.8% seleccionó a WhatsApp, mientras que un 26.6% eligió a Instagram como las redes sociales con las cuales perciben una afectación en sus derechos.

9. ¿El sistema de cámaras de vigilancia del ECU911, puede limitar o vulnerar derechos?



Gráfico 11. ¿El Sistema de cámaras de vigilancia de ECU911 puede vulnerar sus derechos?

Fuente: Investigación de campo (2021).

Elaborado por: Omar Altamirano Villena (2021).

Análisis:

En cuanto a si el Sistema de cámaras de vigilancia de ECU911 puede vulnerar sus derechos, un 36.7% de la población está totalmente de acuerdo, un 18.9% indica que está totalmente en desacuerdo, un 12.5% dice no tener conocimiento sobre esta situación, un 12.2% está de acuerdo, mientras que un 9.1% dice que esta medianamente de acuerdo.

10. ¿Cuáles derechos cree que se restringirían o vulnerarían a través del sistema de vigilancia del ECU911?

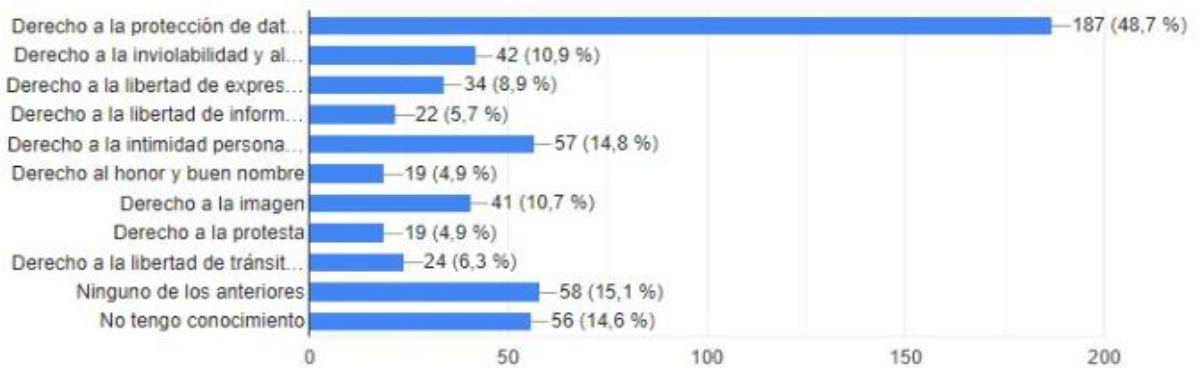


Gráfico 12. ¿Derechos que se vulneran por uso de Sistemas de vigilancia ECU 911?

Fuente: Investigación de campo (2021)

Elaborado por: Omar Altamirano Villena (2021)

Análisis:

En cuanto a cuáles derechos cree usted que se restringirían o vulnerarían con el uso del Sistema de cámaras de vigilancia de ECU911 puede vulnerar sus derechos, un 48.7% indicó que se vulnera su derecho a la protección de datos, un 15.1% dice que no se vulnera ninguno de sus derechos, mientras que un 14.6% afirma que no tiene conocimientos sobre esta situación.

11. ¿Las empresas y/o el Estado, al recopilar datos o información de personas en la web, dispositivos electrónicos y de vigilancia, vulneran o vulnerarían derechos de los ciudadanos?



Gráfico 13. ¿Las empresas del Estado puede vulnerar sus derechos?

Fuente: Investigación de campo (2021)

Elaborado por: Omar Altamirano Villena (2021)

Análisis:

En cuanto a si las empresas y/o el Estado, al recopilar datos o información de personas en la web, dispositivos electrónicos y de vigilancia, vulneran o vulnerarían derechos de los ciudadanos, un 53.1% indicó que está totalmente de acuerdo en esta situación, un 14.6% dijo que estaba de acuerdo, mientras que un 11.7% afirmó que no tenía conocimientos sobre si las empresas del estado o el Estado mismo, al recopilar datos puede vulnerar sus derechos.

12. ¿Cuáles derechos de los ciudadanos cree que se restringirían o vulnerarían a través de las empresas del Estado?

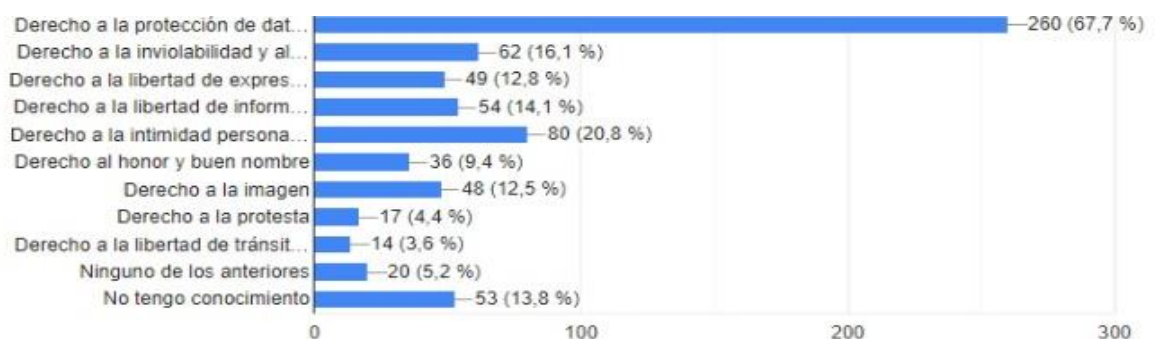


Gráfico 14. ¿Redes sociales por las que puede vulnerar sus derechos?

Fuente: Investigación de campo (2021)

Elaborado por: Omar Altamirano Villena (2021)

Análisis:

Quienes contestaron afirmativamente sobre si las empresas y/o el Estado, al recopilar datos o información de personas en la web, dispositivos electrónicos y de vigilancia, vulneran o vulnerarían derechos de los ciudadanos, un 67.7% considera que se vulnera su derecho a la protección de datos, un 20.8% afirma que se afecta su derecho a la intimidad personal, un 16.1% afirma que su derecho a la inviolabilidad se ve vulnerado.

En rangos menores, se mencionan los derechos a la imagen (12.5%), derecho al honor y al buen nombre (9.4%), derecho a la libertad de tránsito (3.6%) y derecho a la protesta (4.4%).

13. ¿Las empresas que se dedican a recopilar datos o información personal, al venderlas vulneran derechos de los ciudadanos?

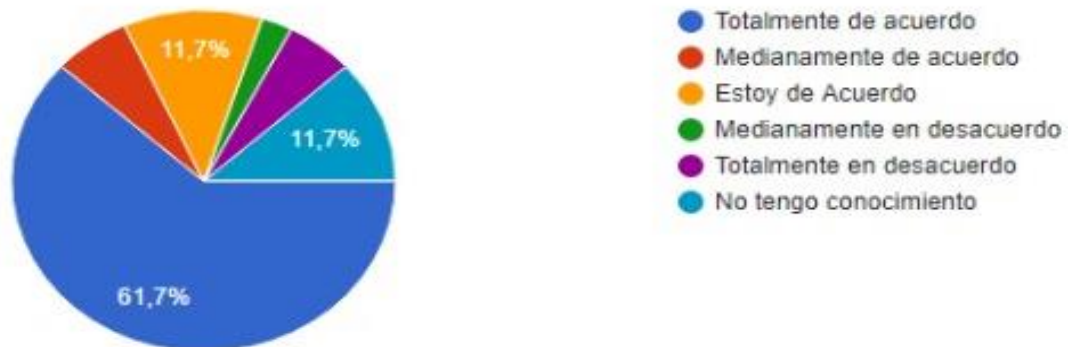


Gráfico 15. ¿Empresas que venden la información pueden vulnerar sus derechos?

Fuente: Investigación de campo (2021)

Elaborado por: Omar Altamirano Villena (2021)

Análisis:

Sobre si las empresas que se dedican a recopilar datos o información personal, al venderlas vulneran derechos de los ciudadanos, 61.7% de ellos indicaron que están totalmente de acuerdo, un 11.7% mencionan estar de acuerdo y un mismo número afirmó que no tenía conocimiento de que las empresas que se dedican a recopilar datos o información personal, al venderlas vulneran derechos de los ciudadanos.

14. ¿Cuáles derechos de los ciudadanos cree que vulnerarían las empresas que se dedican a recopilar datos o información personal, al venderlas?

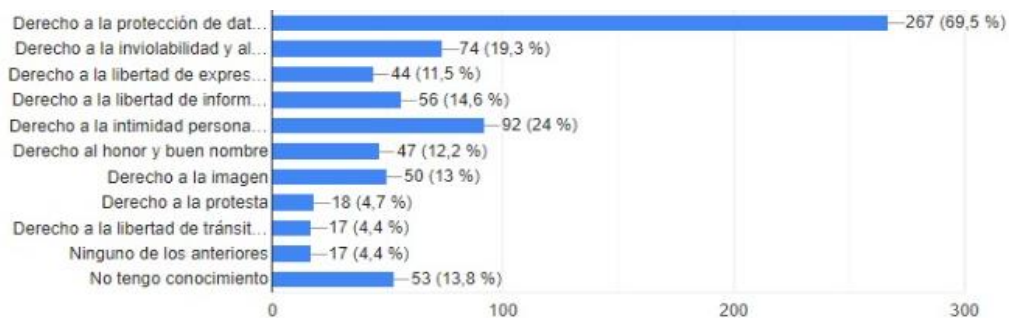


Gráfico 16. ¿Derechos que pueden vulnerar empresas que venden la información?

Fuente: Investigación de campo (2021)

Elaborado por: Omar Altamirano Villena (2021)

Análisis:

Sobre cuáles derechos de los ciudadanos cree que vulnerarían las empresas que se dedican a recopilar datos o información personal, al venderlas, un 69.5% de ellos indicaron que su derecho a la protección del dato, un 24% coincide en que se vulnera su derecho a la intimidad de la persona, mientras que un 19.3% afirma que lo que se afecta es su derecho a la inviolabilidad.

15. ¿Usted considera que, con el avance de la tecnología, deberíamos tener derecho a decidir qué uso se da a la información personal?



Gráfico 17. ¿Derechos a decidir sobre el uso de su información personal?

Fuente: Investigación de campo (2021)

Elaborado por: Omar Altamirano Villena (2021)

Análisis:

Si se considera que, con el avance de la tecnología deberíamos tener derecho a decidir qué uso se da a la información personal, un 69 % afirmó que está totalmente de acuerdo en decidir qué uso tiene su información personal, un 12% indica que no tenía conocimiento sobre lo que hacen o que uso se da la información personal, mientras que un 9.9% indicó estar de acuerdo en conocer y decidir qué uso se le da a su información personal.

16. ¿Usted cree que debería de existir un derecho en el que toda la información que haya generado o compartido sea eliminada de las bases de datos, tanto privadas como gubernamentales?

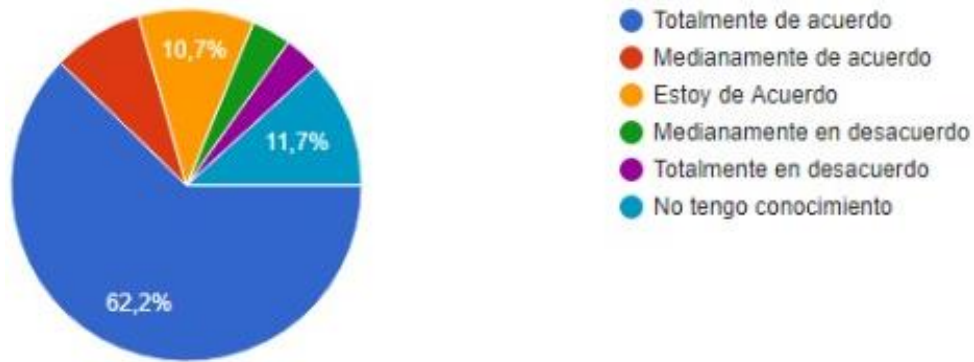


Gráfico 18. ¿Debe haber un derecho para eliminar la información generada o compartida?

Fuente: Investigación de campo (2021)

Elaborado por: Omar Altamirano Villena (2021)

Análisis:

Al respecto de su opinión sobre si debería de existir un derecho en el que toda la información que haya generado o compartido sea eliminada de las bases de datos, tanto privadas como gubernamentales, un 62.2% dijo que está totalmente de acuerdo, un 11.7% dijo que no tenía conocimiento sobre esta situación, mientras que un 10.7% afirmó estar de acuerdo en que toda la información que haya generado o compartido sea eliminada de las bases de datos, tanto privadas como gubernamentales.

17. En una escala del 1 al 10 siendo el 1 lo más bajo y 10 lo más alto. ¿Qué tan capacitadas cree que se encuentran las instituciones públicas del Ecuador para evitar el robo de datos y reaccionar exitosamente para solucionar el problema y proteger la información de sus ciudadanos?

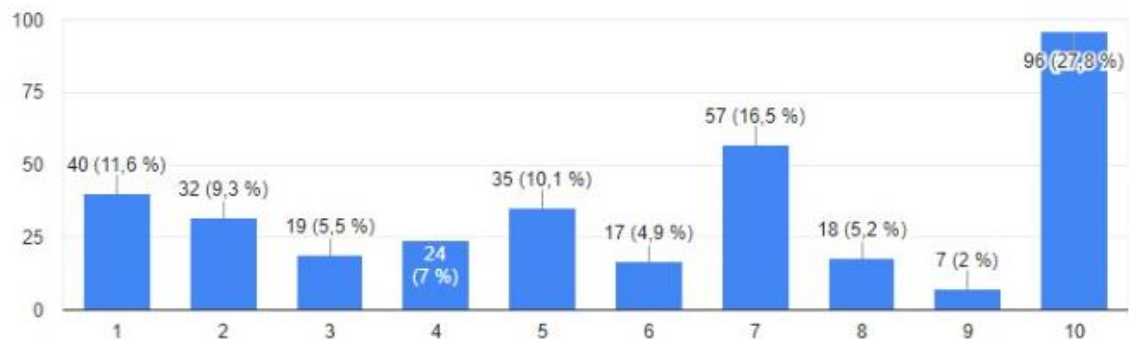


Gráfico 19. Respuesta de las Instituciones públicas frente al ciberdelito.

Fuente: Investigación de campo (2021)

Elaborado por: Omar Altamirano Villena (2021)

Análisis:

Al respecto de su opinión sobre qué tan capacitadas cree que se encuentran las instituciones públicas del Ecuador para evitar el robo de datos y reaccionar exitosamente para solucionar el problema y proteger la información de sus ciudadanos, un 27.8% de los ciudadanos afirmaron que el Estado está capacitado para hacer frente al robo de información. Mientras que un 11.65% de ellos respondió que el Estado no está capacitado para evitar el robo de datos y reaccionar exitosamente para solucionar el problema y proteger la información de sus ciudadanos.

18. ¿Cree usted que la Asamblea Nacional del Ecuador debe de preocuparse por legislar en el área tecnológica que involucre al ser humano, entre ello, el tratamiento de datos personales y seguridad de información personal?

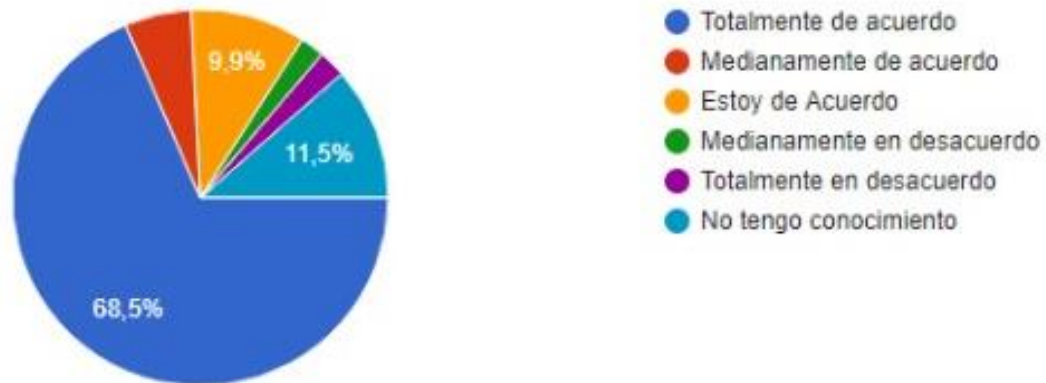


Gráfico 20. Opinión ciudadana sobre la tarea legislativa en el área de tecnología y tratamiento de datos personales.

Fuente: Investigación de campo (2021)

Elaborado por: Omar Altamirano Villena (2021)

Análisis:

Al respecto de su opinión sobre si la Asamblea Nacional del Ecuador debe de preocuparse por legislar en el área tecnológica que involucre al ser humano, entre ello, el tratamiento de datos personales y seguridad de información personal, un 68.5% indicó que está totalmente de acuerdo con esto, un 11.5% afirmó que no tenía conocimiento mientras que un 9.9% dijo que está de acuerdo con que la Asamblea Nacional del Ecuador debe de preocuparse por legislar en el área tecnológica que involucre al ser humano, entre ello, el tratamiento de datos personales y seguridad de información personal.

4.1.3. Análisis e interpretación de los datos recabados mediante entrevista realizada a expertos

- 1. En base al derecho contemplado en el numeral 2 del Art. 16 de la Constitución del Ecuador que determina: "*Todas las personas, en forma propio o combinada, tienen derecho a: El acceso universal a las tecnologías de investigación y comunicación*". ¿Cree usted que su ejercicio tendría como efecto la vulneración de otros derechos de los ciudadanos, contemplados en la Constitución y Tratados Internacionales de Derechos Humanos? ¿Cuáles? y ¿Por qué?**

La mayoría de entrevistados afirmó que no. Entre las principales justificaciones de la respuesta se enlista:

Porque no se visualiza la violación de derechos con el acceso a las TIC, más ayuda a desarrollar tareas en el ámbito educativo y laboral. Lo determinan como una declaración de carácter general que más bien facilita el desarrollo y ejercicio de otros derechos constitucionales. Depende del alcance y si existe a la violación a la intimidad, sino existe, no hay violación de derechos. Debido a que el acceso a tales tecnologías implica el uso de esas plataformas digitales, no se vulneraría ningún derecho de otra persona, esto en virtud que la información personal que decide la persona alimentarla al sistema o plataforma es por cuenta propia. Es decir, que esto es el acceso a las tecnologías, más no a datos privados de otras personas, ya que el usuario debe manejar de manera responsable dicho acceso.

Este acceso puede convertir una persona más productiva generador de ingresos y por lo tanto ayuda a la economía de un país. Además, la información es pública, pero hay grupos de personas que la usan para atentar contra otro ser humano.

Por otra parte, las respuestas afirmativas impusieron su criterio sobre la seguridad y privacidad de la información, las TIC dentro del marco laboral, estudiantil y luego de Covid-19 se ha popularizado y garantizado el acceso universal y privacidad a las tecnologías de información y comunicación para desarrollar las actividades de los

ciudadanos. El derecho a la privacidad se visualiza siempre que se acepten las partes, al estar en las RRSS⁸, queda expuesto y solo el ciudadano decide lo que desea obtener.

Otro de los elementos presentes en las TICs, es Si. Porque la rapidez que caracterizan estas comunicaciones tecnológicas hace que la información se distorsione y pueden afectar el honor de las personas, por encontrarse expuesta su privacidad.

Por otra parte, si se pueden ver afectados los derechos y uno de los derechos en mayor riesgo es a la intimidad, otro es al buen nombre, otro es a la inviolabilidad de correspondencia. La masificación de la gratuidad sin restricciones genera la filtración de información que, por su naturaleza, es sensible con relación a la condición de "persona", de allí que la ausencia de filtros o cláusulas de permisibilidad de uso (que no formen parte de contratos de adhesión), son puertas abiertas (o ventanas al menos) para que terceros potencialmente accedan, usen y exploten dicha información en perjuicio de su titular.

2. ¿Cómo cree usted que las Tecnologías de la Información y Comunicación (TICs), Redes Sociales y aplicaciones tecnológicas, ¿causan o causarían violación de derechos a los usuarios? ¿Cuál sería el proceso para esto?

Para acceder a un programa solicitan una autorización y por lo tanto se debe sujetarse a un contrato de adhesión para su utilización, por lo que está en el usuario el derecho de acceder o no a las mismas. La violación se produciría o se produce por la falta de regulación y control (obviamente enmarcado en la constitución) por lo que estos derechos deben ser armonizados con otros derechos para no afectarlos por ejemplo a algunos detallados en el artículo sesenta y seis de la Constitución del Ecuador.

No creo que causen violación a ningún tipo de derecho, ya que todos tienen derecho a publicar la información que considere, la vulneración de derecho se desarrollaría al exponer información de una tercera persona. Cuando el administrador de tales aplicativos sin consentimiento venda mi información personal o a través de datos. Cuando otras personas o usuarios difunden información que atenta contra la dignidad y la honra de la persona afectada. Cuando por tales aplicativos se proceda a la localización o ubicación de la persona.

⁸ RRSS: Acrónimo de Redes Sociales.

Particularmente porque permiten acceder a las mismas, en algunos casos refugiándose en identidades falsas y que en mucho de los casos resulta difícil o imposible identificar. Es posible que esto ocurra por los llamados hackers, con lo que obviamente debe ser controlado por gente especializada. Sin embargo, si bien creo que debe existir un control, no debería haber una alarma exagerada, porque al fin y al cabo es un delito. Al igual que asaltar a una persona en la calle y robar sus pertenencias, quien hackea invade la privacidad de otra persona. Ambos son actos ilícitos.

Al momento que se permite el uso ilimitado, sin rastro de responsabilidad o identificación fidedigna del consumidor que accede a determinada información a través de las Tics, se crean espacios para que tales sean utilizados libremente. Cuando se usa para victimizar en circunstancias aún no sentenciadas, el uso mediático de las redes y la información puede ser el más grande problema. Por la rapidez y porque hay personas que no reparan en que desconocen algún tema e igual emiten criterios equivocados cuando públicas o tergiversan información que no te pertenece, y para eso existen leyes que lo regulan, lo que se debería hacer es aplicar bien las leyes cuando correspondan, y no por el llamado derecho a la expresión hagan lo que quieran, el problema no es el acceso a la tecnología el tema es lo que haces con ellas, si respetas las leyes y las reglas que existe, no vulnerarías derechos.

Cada persona es responsable de la información dada en sus redes sociales o ingreso de datos a aplicaciones no es una violación si tienes un perfil público y lo compartes, la app tiene niveles de seguridad para tu como usuario te protejas. La filtración de información está sujeta a la seguridad que brindan las empresas encargadas de tener a cargo la administración de la seguridad de la información. Desde el punto de vista cuentas personales: Todas las aplicaciones tienen restricciones y seguridades, las que el propietario debe ser conocedor. Esto restringe el acceso a q otros usuarios "ataquen" al propietario de la cuenta. Se debe capacitar para crear una cuenta en cualquier red social. Desde el punto de vista de que si alguien fue grabado o usado su imagen para causar daño a la integridad, esto debe ser penalizado y aunque en la ley lo define, las personas que difunden esto no tienen conocimiento de la causa. Se debe hacer

campañas de concientización y explicar que pasa en el caso de que alguien viralice algo para hacer un daño a determinada entidad o persona.

3. ¿Qué opinión le merece, el uso que las empresas desarrolladoras de tecnología y el Estado dan a los datos o información obtenida de los usuarios, mediante cualquier plataforma tecnológica? (Desarrolle su respuesta)

La captación de información de los usuarios expone al ciudadano a que sus datos puedan ser utilizados por corporaciones o estados para un control social o venta de información respecto de los gustos de los clientes o usuarios. Es un abuso el que realizan, deben ser normados y regulados. No afecta ni vulneran ningún tipo de derecho, ya que sea compañías de seguridad y comunicación legal mente constituida

Abusiva esto por cuanto el consumidor de tales plataformas tiene la única oportunidad de aceptar las condiciones que llevan implícitas, que si no aceptan las mismas, simplemente no puede usar el servicio. Impidiendo al usuario que pueda sobre ciertas cuestiones inherentes a la persona, esta pueda decidir si la acepta o no. Es también un abuso de la información pues el usuario si bien es cierto se somete a contrato de adhesión al aceptar las condiciones sin embargo se violenta un derecho al otorga la información a terceros.

Mediocre pues no hay seguridad acerca de la confidencialidad debida. Y aunque tecnológicamente exista dicha seguridad, debido a las cláusulas de adhesión de ciertas empresas privadas, se reservan el derecho de transmitir la información de sus usuarios a las demás empresas que forman parte de sus grupos económicos, de manera que el proveedor de telefonía celular que también vende electrodomésticos, y también televisión por cable, internet, etc., les da a todos sus gerentes las facilidades para contactarnos durante sus campañas promotoras de tales bienes o servicios adicionales. Simplemente es invasivo. Al ser Casi ilimitadas, deben tener parámetros de uso que no interfiera en los derechos de los usuarios sin su consentimiento. Es un uso muy amplio, que afecta la privacidad

El estado y la empresa privada, debe garantizar que la información de los ciudadanos que no es pública está segura, pero resulta que la información de teléfonos,

correos que das para una factura por ejemplo ya la tienen para toda campaña de marketing, ventas etcétera tu información se divulga sin ninguna responsabilidad eso no es correcto.

Mientras la información se encuentre protegida estaría bien, debería ser manejada de manera diferente por parte de las mencionadas empresas, debe haber un poco más de restricción por parte de los gobernantes de cada país. La seguridad es deficiente, presenta falencias especialmente en el sector público

Depende lo que estipule el acuerdo que la plataforma desarrolladora pone previo a la aceptación del servicio. Generalmente no lo leen. Es un gran problema eso. Las empresas que desarrollan esto no deben dar la data a nadie mi opinión personal. La tecnología puede tener su avance, pero el Estado no está preparado debido a la corrupción que se ha visto.

La privacidad e integridad de los datos es parte fundamental de cada usuario que da uso de herramientas tecnológicas como aplicaciones, redes sociales, etc. Está bien siempre y cuando no lesione al individuo, y que sea con conocimiento consciente del usuario. La información debe ser privada y se debería regular para que las empresas vendan la información.

4. ¿Cómo experto, que situaciones pueden realizarse con la información o datos recopilados por el sistema de cámaras de seguridad instalada en áreas públicas por el Estado? ¿Esto, podría afectar de alguna manera a los derechos de los ciudadanos?

El desarrollo tecnológico ha llevado a que la humanidad tenga que pagar un precio por el mismo lo que conlleva a que los ciudadanos pierdan parte de su privacidad a través de la recuperación de información. Se afecta el derecho a la libertad, intimidad, libre circulación y de tránsito. Aunque también ayuda a controlar a la delincuencia ya que el Estado es responsable de la seguridad interna y externa y que dado el actual estado de desarrollo tecnológico exige mayores condicionantes que permitan identificar personas para su identificación, localización y ubicación, el estado estaría fijando parámetros mayores de seguridad. Pero éstos si se encontrarían limitados por un

principio de confidencial al uso exclusivo de un gobierno, en dónde no debería difundir abiertamente tales señales o recepción de señales, imágenes, audio voz inherente a la persona en particular, salvo que existiera orden expresa de autoridad pública para que se use tal información, por ejemplo cuando se dan las muertes en la penitenciaría y la forma de sus actos delincuenciales son difundidas a la ciudadanía, no debería de difundirse, sino almacenarse y otorgar a la fiscalía, para uso de particulares fines.

Siendo la persona un sujeto del derecho y de deber jurídico al mismo tiempo su accionar público debe estar dentro de las normas jurídicas a la moral y las buenas costumbres. se pueda establecer mecanismos de control y en la era actual hacer uso de la tecnología lo que estando consciente el ciudadano de ese particular si la información es utilizada solo con esos fines y no distorsionado su uso no afectaría a derecho alguno. Tanto más que para fines de investigación se debe de realizar con las partes procesales. Las áreas públicas están expuestas al control. Es posible que surja alguna afectación, pero ese dependería de cada caso en particular, ya que también contribuye al control de seguridad ciudadana

5. Cuál es su opinión sobre el uso que se podría dar a los datos que recolectan las Empresas y el Estado. ¿Tiene alguna consecuencia negativa en relación a los derechos de los ciudadanos?

Repercute directamente en el derecho a la intimidad y a una posible utilización de dicha información para fines que atenten contra la dignidad de las personas o su integridad física inclusive la vida. No existe transparencia en el uso de la información, hasta que los ciudadanos activan el aparato judicial por verse afectados. No creo que se vulneren derechos. No afectaría a la persona ni a la identidad de ésta, la información nace de la persona y el estado es responsable de conservar y guardar la información proporcionada.

Es el uso exclusivamente relacionado a la actividad o servicio que prestan, cumpliéndose con la obligación de mantener la reserva de la obligación. Cuando su uso es ilimitado sin fines establecidos previamente, pueden afectar negativamente, sin embargo, existe información que corresponde a la transparencia que deben aplicar las empedas d instituciones estatales. Se debe identificar la información, el sujeto y el uso

El mal uso que se pueda dar es infinito, una vez que tus datos son público le sirve a la gente q se dedica a extorsionar, bandas delictivas, te dejan expuesto a diversidad de eventos, las consecuencias son graves no tienes tranquilidad y vives desconfiando de todo. Lo negativo es que exista una fuga de datos, pero para esto en los contratos labores se deben incluir de forma clara y detallada que aspectos deben guardarse y no compartirse.

Su uso debe ser confidencial y especialmente destinado al análisis de información más no a la divulgación de la información. Pienso que no, debido a que, en términos tecnológicos a esto se lo conoce como Big Data y la misma ya se está aplicando en todas las grandes plataformas que hay. La Big Data nos permite hacer el estudio del comportamiento de las personas. Si hubiese la certeza, lo cual es muy difícil que se dé, y se utiliza esta información para cuestiones como: salud, turismo, consumidor y afines; entonces valdría la pena. Pero imaginemos que la Big Data la usen para malas acciones, entonces sería catastrófico.

La vulnerabilidad de los datos. Si, toda información de terceros que sea difundida sin autorización es una violación a la seguridad y privacidad de cada usuario. Esta data debería ser bien resguardada para que no caiga en manos de delincuente; y tampoco debe ser usada para fines políticos. Las bases de datos de las personas deben servir para implementar programas de capacitación

6. Cómo usuario de internet y redes sociales, cree que la información o datos personales proporcionada por usted, ¿serviría para se configure la violación de sus derechos? ¿Cuáles derechos sería y por qué? (Desarrolle su respuesta)

Si, porque a través de estos algoritmos que manejan estas super computadoras permiten establecer patrones de conducta, frecuencias en cuanto a gusto de las personas. Si, por no haber transparencia ni información de mis datos personales. Si, puesto que se violenta particularmente el derecho a la privacidad a no interrumpir su horario de descanso y tranquilidad. Es posible que ocurra. Aún en el caso, de que la empresa que recolecta mis datos no tenga intención alguna de violar mi derecho de privacidad y de compartirlo con otras personas, siempre existe la posibilidad de que alguna persona proceda de modo inadecuado. Éste es un punto muy delicado sobre en quien recae la

responsabilidad, cuando ocurre una violación a la privacidad ocasionada con un tercero, ya que es difícil determinar si hay culpabilidad por no cuidar bien de la información o si la habilidad del tercero excede cualquier medida razonablemente aceptable.

Podría ser violatorio cuando se use sin consentimiento y para fines legalmente no establecidos. El derecho a la propiedad, a la seguridad, el buen vivir, entre otros derivados de ellos, por ejemplo cuando se proporciona información del Domicilio y puede ser publicada poniendo en riesgo la seguridad y el acceso a la delincuencia, , partiendo de aquello, varios delitos que pueden ser perpetrados con Información que se filtra para usos indebidos. Podría darse, pero para mí las redes son solo espacios sociales que uso sin prudencia por mi actividad laboral.

En cuanto a las redes sociales la gente la usa como un medio de comunicación pero todo lo que está en la web es utilizada para diferentes temas como campañas de marketing que de acuerdo a tus like en publicaciones ya te envía sugerencia de amistades, cuentas a seguir, paginas a visitar, ya que las multinacionales trabajan con los datos de la red, compran data par su marketing, pero también hay gente que utiliza estos datos que las mismas personas publican par chantajes o para estafas, ya depende de cada persona cuidar q publica así evitarían en algo las vulneración de sus derechos

No, porque la información debe ser almacenada bajo las normas de seguridad correspondientes

Si considero que las empresas que obtienen nuestros datos si invaden nuestra privacidad y además ellos se benefician económicamente o de cualquier manera q ellos consideren oportuno, Manejando los protocolos de seguridad no hay violación alguna. Si, por que tendrían acceso a toda mi información violando mi privacidad. Derecho a la confidencialidad de la información estipulado en la constitución política del Ecuador

La respuesta es no, porque si yo estoy proporcionando mi información, es porque se dónde la voy a colocar. En caso de que la empresa en donde proporcioné mis datos los haga públicos para que sean vulnerados, tomaría acciones legales. Si yo publico algo personal, al hacerlo público, estoy asumiendo el riesgo. Recalco, si la empresa infringe, el derecho que se viola es el de la privacidad y dependiendo de que pase con los datos,

se generaría una cadena de violación de derechos de diferentes tipos. Todo dato que se proporcione está sujeto a violentarse. Definitivamente, por eso lo expresado en puntos anteriores en el sentido de que la información recopilada debe contar con todas las seguridades del caso. Si mis datos personales son empleados de mala manera si se violan los derechos de privacidad.

7. ¿Cree que la práctica de recolección de datos mediante cookies o métodos de captación de información adicional es indiscriminada, al recopilar datos sin conocimiento ni consentimiento del usuario? ¿Qué puede provocar?

Los mecanismos tecnológicos pueden servir para robo de información que atente contra el derecho a la intimidad. Debe ser una autorización expresa. Es indiscriminada porque es ahí cuando el usuario o el consumidor se ve limitado de rechazarlas o aceptarlas, en caso de no estar de acuerdo de aceptar no puedo usarla. Por lo general se observa páginas que advierten al usuario que están utilizando cookies. éste es un modo de prevención implantado en internet, justamente para evitar que se recolecten datos sin aprobación del usuario

Además, provoca invasión de espacios privados como el descanso, o el mismo trabajo. Gracias a sus algoritmos de focalización de tendencias consumistas, contactan por varios medios a los usuarios para ofrecerles bienes o servicios no requeridos, es decir ejercen presión para que el usuario adquiriera obligaciones con consentimiento inducido. Una de las causas, se debe a la falta de control de la obtención de información y la adecuación legal a esta gran industria del internet, aún hay muchos modos/ delitos que no constan en la legislación y deben ser considerados para limitar dicho acceso ilegal

Se considera que es indiscriminada pero también los usuarios son imprudentes y lo permiten, luego pueden interpretar que es violación de su vida privada, esto puede provocar que reciba notificaciones de todas las empresas que compraron esa data para su marketing, provocar que te asalten en la entrada de tu casa porque publicaste tu dirección completa, estas expuesto a infinidad de situaciones.

Ellos manejan buenas estrategias de marketing muy persuasivas y manipuladoras que sutilmente obtienen los datos, supuestamente ellos piden consentimiento, pero esto es algo estratégico que a veces no se dan cuenta que lo hacen. Esto generaría desconfianza al uso de las tecnologías, porque existen datos que pueden facilitar a terceros para causar daño a cualquier persona dañando su buen nombre u obtener información confidencial como claves y contraseñas. La recolección de datos mediante cookies afecta la privacidad y puede exponer a los usuarios.

8. Para el usuario, ¿Qué consecuencias traería la recolección de sus datos por parte de empresas y entidades gubernamentales? ¿Conoce el proceso?

Entre las respuestas se obtuvo como principal consecuencia, la pérdida del anonimato, el abuso de información personal, porque no tiene ni goza de consentimiento, si se siente vulnerada activaría los mecanismos legales. Ellos captan datos de distintas fuentes, usurpando información porqué dan inicio a una actividad en dónde la recolección de información obedece a implementar otros procedimientos para recopilar información focalizada. Pueden ser víctimas de un hackeo. Aunque otras consecuencias pueden ser que el dato se use para capturar delincuentes o usados para perseguir opositores del gobierno o para perseguir a un enemigo político podría alegarse que éste ha cometido un delito. Implica el riesgo de exposición política, mediática, o ante organizaciones delincuenciales.

Se entiende que la información del estado es pública por ello si la persona está consciente de ello, sabrá las consecuencias a futuro. Las consecuencias son muchas, entre ellas pueden ser manipular y hacernos comprar cosas no deseadas, en tema político puede hacer votos por algún candidato que no queremos.

Todo usuario es un ciudadano, y todo ciudadano, debe rendir cuentas al país. Por ende, todos de una forma u otra, acceden a plataformas gubernamentales para realizar diferentes trámites. Mientras la data sea del tipo que es necesaria para el gobierno de turno, entonces, estaría correcto. Para algo diferente a esto, no debe de producirse. Por ejemplo: El SRI, sabemos que debemos declarar facturas y no se lo hace como debe de ser. Por ende la entidad trae como consecuencia una multa. (la misma que puede ser desviada por corrupción). Aunque la recolección de datos por parte de empresas o del

Estado como los Censos ayuda a la planificación, pero debe ser empleada de manera responsable.

9. ¿Tiene conocimiento si la recolección de información de datos digitales está normada legalmente por el Estado Ecuatoriano?

La recolección de información de datos digitales no está normada, todo el acceso a internet no está regulado, existiendo una responsabilidad ulterior, falta regulación normativa por parte de la Asamblea Nacional. No se encuentra mayormente legislado a nivel nacional, tiene que ser más específica y protectora. Hay cosas insípidas, pero no es una normativa completa y suficiente, lo poco que está normado no se lo aplica eficientemente. Por ejemplo, las distintas llamadas a mi teléfono ofreciéndome productos. Se supone que todas las entidades públicas, por ejemplo, pueden recolectar la información y solo pueden usarla para los fines institucionales. Las privadas se fundamentan en el consentimiento forzado que el usuario brinda en los contratos de adhesión.

Al respecto, si hay delitos establecidos, relacionados, en el COIP con actos de uso indebidos o alteraciones de sistemas y datos. Es posible que con la teoría del caso adecuado, se ajuste a esos delitos Normandos en la legislación penal ecuatoriana

La gran mayoría de los entrevistados puntualizó que la norma es deficiente deberían de ser reguladas, que si esta es poca y no tiene la cobertura para todos los intereses del ciudadano y del consumidor final. El avance de la tecnología es una de las situaciones que le ganan a cualquier legislación vigente, entre lo que hay que normalizar son compras en el exterior, retención de IVA, impuestos.

10. ¿Cree usted que el Estado Ecuatoriano debería de normar el uso, captación y venta de datos de usuarios por parte de la Empresas desarrolladoras tecnológicas y de las entidades gubernamentales?

La gran mayoría de los entrevistados coincide en que la información de los ciudadanos no podría estar en manos de personas particulares que hagan uso comercial de las mismas, todos son expuestos al uso de su información personal, se considera que debe ser normada porque violan su intimidad, llegando hasta desarrollarse el acoso.

Debería de ser más transparente la entrega de éste tipo de datos para conocer, quién los entregó y quién los recibió, así mismo debería de existir suficiente información que indique en qué lugar se puede encontrar al que está haciendo uso de la información de manera que pueda responder de ser necesario, a esto debe de agregarse la agilidad en el proceso respectivo de reclamo.

Otra de las opciones que deben normalizarse, es que debe tutelar la opción de negarse a compartir información irrelevante como aquellos detalles sobre si los bienes inmuebles deben ser inscritos en el registro de la propiedad donde se encuentren, la entidad que desea saber información al respecto, debe hacer su gestión investigativa, y promover la eficiencia en la interacción entre entidades públicas, v.g. municipios, registradores, entes de control. Se debe empezando por normalizar la captación de datos y deben estar en continua actualización y mejoras, ya que siempre las empresas buscaran evadir las reglas.

11. ¿Considera que el desarrollo de las TIC, software y programas como la inteligencia artificial podrían vulnerar derechos? Cuáles y por qué?

Entre los principales derechos vulnerados pueden ser: la vulneración de derechos, como el derecho a la intimidad, honra y buen nombre, merece un mayor control a efecto que exista una limitación consentida por el usuario, persona o ciudadano, responsables sobre la salud, el uso de las infinidades de aplicaciones afecta la salud del ser humano

Los avances tecnológicos por el alcance pueden violentar particularmente el derecho a la privacidad e intimidad. La inteligencia artificial (IA) ha evolucionado demasiado, al punto de que se alimenta con Big Data, que refieren al estudio de comportamiento, como una de tantas opciones de uso. Por ende, las tecnologías simplemente actúan basadas en patrones y, aunque no estoy seguro de que sea un derecho, se violaría el libre albedrío; ya que habrá un determinado momento, en donde algo que siempre realizo, ya no lo pueda hacer y sin embargo, la tecnología lo hizo sin mi consentimiento.

12. En su opinión, ¿Cuál sería, la forma óptima y segura de utilizar las TIC, Redes Sociales y Aplicaciones tecnológicas? para evitar la captación de nuestra información y no ser víctimas de vulneración de derechos?

Es necesario eliminar mecanismos que no permitan rastrear a los ciudadanos. Que la adquisición y uso de las plataformas deba ser autorizado de forma expresa, conociendo en todos los detalles de la información que va hacer usado por las empresas y estado. No existe una forma segura de utilizar ya que el problema no es elevar información, sino que existen personas, ya sean los que trabajan en las empresas tecnológicas o hackers que hacen mal uso de los datos personales.

Ser consciente de la información que publiquemos. Ser responsable de las claves de acceso a los aplicativos que dispongo o uso. Conservar respaldos de los formularios y de las cookies que he autorizado a efecto de conocer a ciencia cierta llegado el momento apropiado que es lo que he autorizado y de qué forma.

No creo que haya manera de hacerlo, el humano es un ser sumamente inteligente y siempre va a encontrar la manera de ir más allá de lo que permiten las regulaciones. Por otro lado, la imposición de normativas siempre es lenta, debido a la cantidad de procesos que tienen que pasarse antes de ser aprobadas. Los hechos siempre llegan antes que el derecho. Bajo la legislación amplia y clara sobre su uso, y bajo la autorización de cada individuo, para fines estatales y legales, limitando su uso y supervisando la información que contenga, sería la manera más óptima de utilizar las TIC. El internet y las redes sociales son un gran poder, puede ser muy beneficioso es verdad, nos permite estar actualizados y tener noticias en segundo la, pero en manos equivocados puede generar incertidumbre y gran daño social.

En ese contexto, se insiste en que los usuarios no suministrar datos e información sensible que pueda causar conflictos de privacidad y el estado debe de normar esto para que en caso de vulnerabilidad de información se pueda dar opción al ciudadano de hacer su reclamo. Que exista una huella ética en cada individuo a través de la capacitación y consecución consciente de los puntos vitales buenos y malos del uso de este derecho. Las cuentas de las redes sociales deben ser autorizadas por parte del Registro Civil para que no haya perfiles falsos.

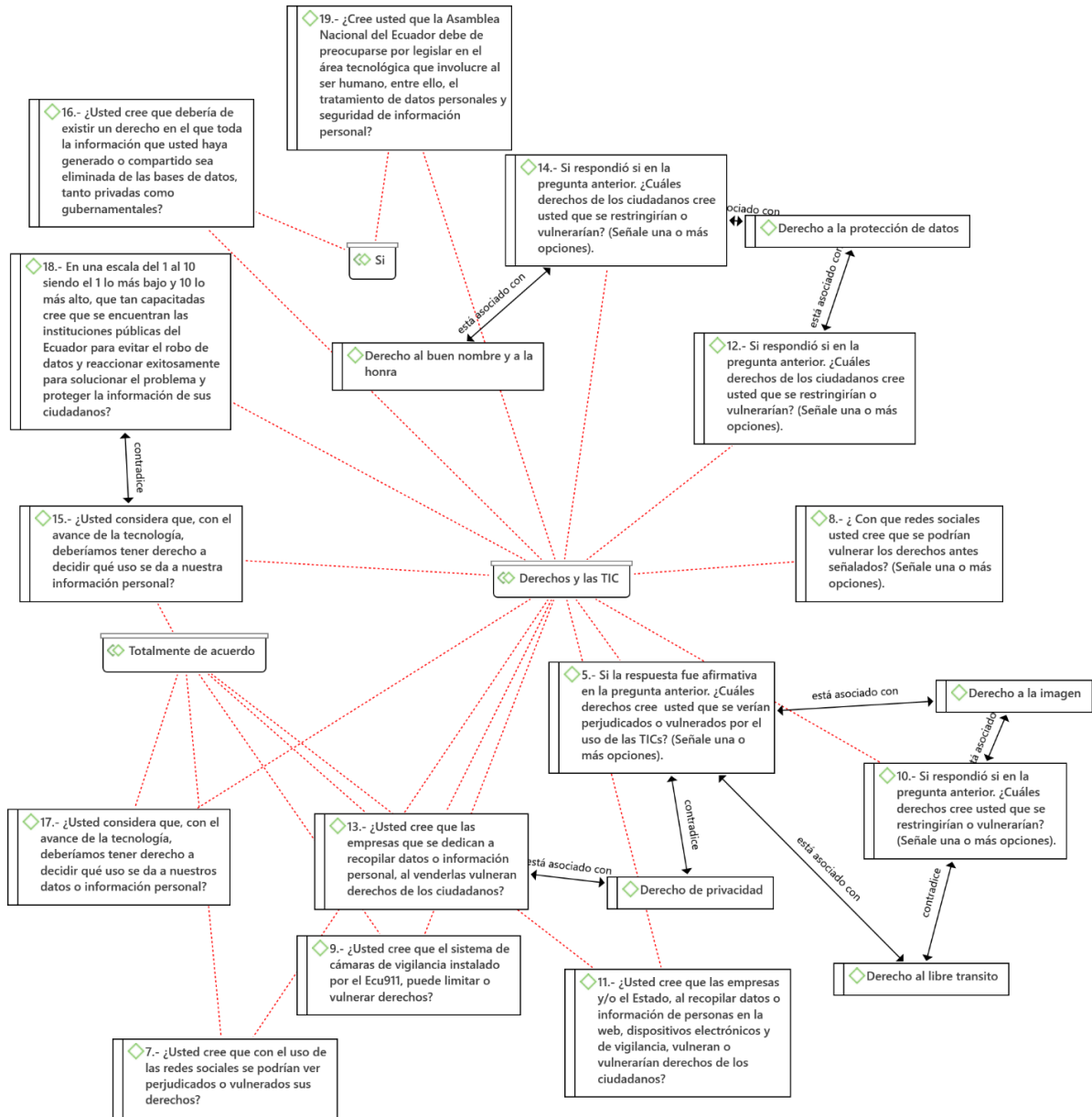


Gráfico 21. Red de resultado de la encuesta aplicada.

Fuente: Investigación de campo (2021) Atlas. TI.

Elaborado por: Omar Altamirano Villena (2021)

4.1.4. Conclusiones.

Como principal conclusión dentro de la encuesta se ha determinado que la muestra se caracterizó por realizarse entre personas comprendidas entre veintiún (21) y cuarenta (40) años (69.3%), de sexo femenino (51%), formación educativa de tercer nivel (51%).

Estos tienen la percepción que las TICs son un mecanismo por donde se podría ver perjudicados o vulnerados sus derechos (47.9%), donde los principales medios usados son los smartphones (65.4%), que entre las principales redes sociales han identificado a Facebook (76.3%) y WhatsApp (63.8%), consideran además que el uso del Sistema de cámaras de vigilancia de ECU911 puede vulnerar sus derechos (48.7%) y también las empresas que se dedican a recopilar datos o información personal, al venderlas vulneran derechos de los ciudadanos (61.7%).

Entre los derechos que consideran vulnerados o afectados, sienten que sus derechos a la protección de datos privados se ven vulnerada con las TICs (66.7%), con el uso del Sistema de cámaras de vigilancia de ECU911 (48.7%), al recopilar datos o información de personas en la web, dispositivos electrónicos y de vigilancia (67.7%), las empresas que se dedican a recopilar datos o información personal, al venderlas (69.5%).

La población quiere decidir qué uso se da a la información personal (69%), considerando además que debería de existir un derecho en el que toda la información que haya generado o compartido sea eliminada de las bases de datos, tanto privadas como gubernamentales (62.2%). Aunque las garantías son pocas ya que pocas instituciones públicas del Ecuador para evitar el robo de datos y reaccionar exitosamente para solucionar el problema y proteger la información de sus ciudadanos equivale al (27.8%), por ello están totalmente de acuerdo en que la Asamblea Nacional del Ecuador debe preocuparse por legislar en el área tecnológica que involucre al ser humano, entre ello, el tratamiento de datos personales y seguridad de información personal (68.5%).

Al respecto de la entrevista realizada a diversos profesionales, en base al derecho contemplado en el numeral dos del artículo dieciséis de la Constitución del Ecuador, cree usted que su ejercicio tendría como efecto la vulneración de otros derechos de los ciudadanos, contemplados en la Constitución y Tratados Internacionales de Derechos Humanos, la mayoría afirmó que no determinan como una declaración de carácter general

que más bien facilita el desarrollo y ejercicio de otros derechos constitucionales, la información personal que decide la persona alimentarla al sistema o plataforma es por cuenta propia ya que el usuario debe manejar de manera responsable dicho acceso. Este es el mecanismo con el que coincidieron la mayoría, de cómo cree usted que las Tecnologías de la Información y Comunicación (TICs), Redes Sociales y aplicaciones tecnológicas, causan o causarían violación de derechos a los usuarios.

Se afirma que no causen violación a ningún tipo de derecho, ya que todos tienen derecho a publicar la información que considere, la vulneración de derecho se desarrollaría al exponer información de una tercera persona. Cuando el administrador de tales aplicativos sin consentimiento venda mi información personal o a través de datos.

Cuando otras personas o usuarios difunden información que atenta contra la dignidad y la honra de la persona afectada. Cuando por tales aplicativos se proceda a la localización o ubicación de la persona. La filtración de información está sujeta a la seguridad que brindan las empresas encargadas de tener a cargo la administración de la seguridad de la información. Pero en el caso de cuentas bancarias personales, todas las aplicaciones tienen restricciones y seguridades, las que el propietario debe ser conocedor.

La captación de información de los usuarios expone al ciudadano a que sus datos puedan ser utilizados por corporaciones o estados para un control social o venta de información respecto de los gustos de los clientes o usuarios. Es un abuso el que realizan, deben ser normados y regulados. No afecta ni vulneran ningún tipo de derecho, ya que sea compañías de seguridad y comunicación legal mente constituida, aunque coinciden también en que el estado y la empresa privada, debe garantizar que la información de los ciudadanos que no es pública está segura, pero resulta que la información de teléfonos,

como el sistema de cámaras que son necesarias para otros beneficios ciudadanos. Reconocen además que los derechos son vulnerados o afectados por la propia iniciativa ciudadana al permitir o no leer las instrucciones que los dispositivos o aplicativos tecnológicos le indican a la hora de usarlos. Lo que deja sin garantías de protección al usuario o consumidor final.

4.1.5 Discusión

Una de las grandes empresas de telecomunicación como Telefónica (2016), menciona que el respeto de las empresas por los Derechos Humanos comenzó a ganar importancia en los años noventa, aunque no ha sido hasta 2011 cuando se ha establecido un estándar internacional de referencia: los Principios Rectores de Empresas y Derechos Humanos de las Naciones Unidas en 2011. Por tanto, el sector TIC juega un importante papel en la promoción de los Derechos Humanos impulsando el desarrollo económico, mejorando aspectos como la calidad de vida, el acceso a la educación, la protección del medio ambiente y facilitando el desarrollo de la sociedad de la información.

En este contexto, es necesario resaltar que uno de los resultados obtenidos de la investigación se centra en los derechos que se pueden ver afectados por las TIC, sin embargo, es necesario evaluar lo que incide de manera positiva y lo que es negativo hacia las personas y su privacidad o derechos relacionales. Al respecto Rico (2012), indica que, aunque en el lenguaje común se suele hablar de Facebook, Tuenti, u otras, etc. como una red social, lo cierto es que estas son las empresas que prestan los servicios para la instalación de la plataforma electrónica donde funciona la red social; en su condición de prestadores de servicios de la Sociedad de la Información, estas empresas están sometidas a un régimen jurídico específico.

Por otra parte, entre los resultados obtenidos, se identificó que las principales fuentes de control son el Estado y por otra parte la empresa privada, esta conjetura tiene mucho sentido de orden ejecutivo, ya que son ellos los que deben normar la actuación de la sociedad sobre el acceso a datos e información. Al respecto Romi Mukherjee (2018), infiere que un enfoque de derechos humanos en la ciencia, la tecnología y el desarrollo busca llamar la atención sobre la forma en la que la comunidad internacional se relaciona con los desafíos globales urgentes. Este concepto ingresó en el léxico de la ONU en 1997, con el pedido de Kofi Annan de que los derechos humanos se integraran a los mandatos, la gestión y las metodologías para el desarrollo y la cooperación internacional de las Naciones Unidas.

En este contexto, los países miembros de las naciones unidas aportan con el desarrollo del marco normativo que debe regular sus acciones en cuanto a las TIC y los derechos humanos en general. Rico (2012) menciona que el ejercicio de la libertad de expresión en Internet ha sido objeto de preocupación constante, a tal punto que en junio de 2011 Naciones Unidas (ONU), la Comisión Interamericana de Derechos Humanos (CIDH), la Organización de Estados Americanos (OEA), la Organización para la Seguridad y la Cooperación en Europa (OSCE) y la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP) firmaron la Declaración Conjunta sobre la Libertad de Expresión en Internet (DCLEI) donde se establecen los principios aplicables a la libertad de expresión en este entorno.

Las bases de la DCLEI también imponen a los Estados la obligación de promover el acceso universal a Internet para garantizar el disfrute efectivo del derecho a la libertad de expresión, indicando que "...el acceso a Internet también es necesario para asegurar el

respeto de otros derechos, como el derecho a la educación, la atención de la salud y el trabajo, el derecho de reunión y asociación, y el derecho a elecciones libres”. En esta situación, se hace meritorio expresar que el consentimiento del usuario es necesario, pero no obligatorio en algunos casos, como en el de la Seguridad pública que ejerce la Policía Nacional a sus compatriotas.

González (2016), en su investigación Privacidad en internet: los derechos fundamentales de privacidad e intimidad en internet y su regulación jurídica. La vigilancia masiva, afirma que los gobiernos también se han beneficiado con la utilización de estas tecnologías permitiendo una mejora considerable en la atención de sus fines y objetivos. Sin embargo, estos también han aprovechado dichas tecnologías, particularmente la vigilancia electrónica, para combatir el terrorismo y otros delitos, que termina también afectando la intimidad y la privacidad de las personas. La actividad desplegada por algunas agencias de inteligencia pareciera que se ha desarrollado con base en una cuestionable legislación adoptada ante la urgencia y necesidad de combatir actos terroristas, lo que ha permitido el acceso a las comunicaciones y los documentos privados de las personas con el objetivo de proteger la seguridad interna de las naciones.

Rodríguez Álvarez a través de la Agencia Española de protección de datos (2021), afirmó que Internet tiene "una capacidad de almacenamiento y difusión potencialmente ilimitada de la información que puede repercutir en la vida de los ciudadanos", y que la forma en la que se afronten estas cuestiones determinará el tipo de sociedad que construimos, “una en la que los individuos puedan desarrollarse libremente o una en la que el recuerdo permanente y la conciencia de que todo queda registrado condicione el libre desarrollo de la personalidad”. En este sentido, la investigación aborda la necesidad

de establecer una propuesta conciliadora para que impulse y promueva la normativa de acceso a la información y datos. Así como los derechos que tienen los ciudadanos y la sociedad.

4.1.6 Comprobación de hipótesis

La hipótesis declarada al principio de la investigación afirma que el uso de las TICs, vulneran los derechos de los ciudadanos ecuatorianos, por la deficiente legislación que regule el tratamiento de datos.

Como se pudo observar en el análisis de las encuestas a la muestra seleccionada, se pudo evidenciar que existe vulneración a los derechos de los ciudadanos ecuatorianos, siendo el uso de telefonía móvil un canal con mayor recurrencia en quejas y por la que más del 60% de los usuarios inquieren una regulación sobre el uso que se le da a la información personal que estas grandes empresas tienen.

CAPITULO V

LA PROPUESTA DE INTERVENCIÓN

5.1. Introducción

La necesidad de establecer normativas y estandarizar los procedimientos, procesos y sistemas de información en general que usan los ciudadanos ecuatorianos, permite evidenciar que existe un gran número de elementos y derechos que son violentados o vulnerados en varias formas sobre el acceso y la captación del dato o información personal de los ecuatorianos o de aquellas persona que usan tecnología para entreteniendo u operar de buena fe con el uso de plataformas tecnológicas, ya sea en el sistema financiero, económico o productivo de la República de Ecuador.

La encuesta aplicada dentro del estudio muestra que los ciudadanos se sienten perjudicados o vulnerados en sus derechos (47.9%), donde los principales medios usados son los smartphones (65.4%), que entre las principales redes sociales han identificado a Facebook

(76.3%) y WhatsApp (63.8%), consideran además que el uso del sistema de cámaras de vigilancia de ECU911 puede vulnerar sus derechos (48.7%) y también las empresas que se dedican a recopilar datos o información personal; al venderlas o transferirlas vulneran derechos de los ciudadanos (61.7%).

Entre los derechos que los ciudadanos consideran que se encuentran vulnerados o afectados, puedo determinar que es el derecho a la protección de datos privados, el mismo se vulnerada con el uso de las TICs en (66.7%), con el uso del sistema de cámaras de vigilancia de ECU911 (48.7%), al recopilar datos o información de personas en la web, dispositivos electrónicos y de vigilancia (67.7%), las empresas que se dedican a recopilar datos o información personal para venderlas o transferirlas en un (69.5%).

Estos eventos, siendo que se repiten cada vez con mayor frecuencia, mantuvo un espacio reducido de discusión a nivel de la función legislativa, creando la novísima ley orgánica de protección de datos personales, la misma que otorga un plazo de dos años para la implementación y adaptación por parte de las empresas que se dediquen al tratamiento de datos. Siendo mucho menos la discusión de la temática a nivel gubernamental o entiéndase por la función ejecutiva, con el fin generar y establecer políticas públicas, que incentiven al estudio y creación de normativa que regule la captación de datos, su uso y el intercambio.

La propuesta de transparencia en el tratamiento de datos, necesariamente debe venir de la sociedad civil, ya que sus derechos se encuentran en juego, para lo cual debemos exigir que se realice una real intención de lograr la transparencia y democratización de los datos que fluyen en los canales públicos y privados, ya sea para el ámbito de análisis estatal o comercial, con el fin que permita un escalamiento, existiendo la discusión entre los intervinientes, siempre con el fin de hacer prevalecer los derechos constitucionales de los ciudadanos.

Los mecanismos de vigilancia ciudadana que se lleva a cabo con el acceso a datos personales desde el sector empresarial que capta los datos, así como los que se dedican al área del marketing y publicidad, desde las redes sociales y en general desde el uso de dispositivos móviles o de las TICs implican procedimientos o acciones que no son abordadas por el consumidor final, ya sea por falta de conocimiento o por falta de iniciativa gubernamental de hacerlo público, conllevando a consecuencias que afectan la privacidad de la persona y el derecho a mantener su vida íntima en un ambiente de paz y seguridad.

Con este antecedente, y considerando que la Constitución de la República, en su numeral dos del artículo dieciséis de la Constitución de la República del Ecuador que determina: "Todos los ciudadanos, en forma individual o colectiva, tienen derecho a: El acceso universal a las tecnologías de información y comunicación", en concordancia con la novísima Ley Orgánica de Datos Personales vigente desde su publicación en el Registro Oficial, es decir desde el veintiséis de mayo del dos mil veintiuno, implicando la protección por parte del Estado, para que se haga efectivo éste derecho, sin tener consecuencias negativas para los ciudadanos.

5.2. Objetivo

Con el fin de evitar las vulneraciones de derechos, el objetivo es constituir o crear la Agencia de Protección de Datos Ecuatoriana (APDE), que contribuya a la aplicación coherente de las normas de protección de datos en todo el territorio nacional, promueve la cooperación interinstitucional, así como público privado y sobre todo la aplicación del régimen sancionatorio en protección y defensa de los derechos constitucionales.

5.3. Factibilidad

Considerando la vigencia de la Ley Orgánica de Protección de Datos, con su posterior aplicación del régimen sancionatorio y la consecuente elaboración para posterior aplicación del

Reglamento a la Ley Orgánica de Protección de Datos: la normativa es factible de implementarse, siempre y cuando sus instituciones gocen de independencia y presupuesto independiente, con el fin de aplicar la normativa e impulsar mecanismos legales que contempla la legislación interna, con el apoyo de la función judicial y demás entes gubernamentales.

5.4. Descripción

La propuesta de la entidad llamada Agencia de Protección de Datos Ecuatoriana (APDE), debemos describirlo cómo un organismo ecuatoriano independiente, con presupuesto autónomo, que se encargue de velar por el cumplimiento del derecho constitucional a la privacidad de los datos de los ciudadanos y ejercer su protección, conforme lo determinado en la Ley Orgánica de Protección de Datos Personales, además de ello de ello al detectar delitos, tenga la capacidad de informar a la Fiscalía, siendo parte procesal. Este organismo debe actuar por denuncia expresa de los ciudadanos, a petición de parte o de oficio.

La Agencia de Protección de Datos Ecuatoriana (APDE), deberá estar representada por el Superintendente de la Agencia de Protección de Datos, conforme lo determina el artículo setenta y siete de la Ley Orgánica de Protección de Datos Personales. Además de ello contará con la autoridad de protección de datos que ejercerá conforme su competencia, funciones y atribuciones determinada en el artículo setenta y cinco y setenta y seis de la LOPDP, su actividad estará enmarcada con el fin de ejercer control y capacidad para investigar infracciones que se contrapongan al derecho de protección de datos de los ciudadanos o personas jurídicas ecuatorianas.

Se deberá contar con el inspector de protección de datos personales; el mismo que cumplirá con el rol de realizar inspecciones, de oficio o a petición de parte, a las entidades y empresas que desarrollaren el tratamiento de datos, con el fin de velar que se cumpla con la

normativa vigente y evitar la vulneración de derechos constitucionales, estando bajo la autoridad de protección de datos, informará sobre las contravenciones observadas.

La Agencia de Protección de Datos Ecuatoriana (APDE), estará compuesta por tres órganos, el ejecutivo, administrativo y el jurisdiccional.

El órgano ejecutivo asumirá la representación legal, por medio del Superintendente de la agencia.

El órgano administrativo estará integrado por un cuerpo colegiado, compuesto por el Superintendente de la agencia, la autoridad de la Dirección Nacional de Registro de Datos Públicos (DINARDAP) y la autoridad del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL).

Las competencias del cuerpo colegiado, sería la capacidad de expedir actos administrativos, normativa interna, resoluciones institucionales y jurisdiccionales, salvaguardando que se encuentren con apego a la normativa constitucional y legal vigente de la materia.

El órgano jurisdiccional estará integrado por la Autoridad de Protección de Datos y el cuerpo colegiado. Las actividades a desempeñarse según su competencia, asumiría la autoridad de protección de datos, resolvería impugnaciones administrativas, quejas y denuncias, cómo ente de primera instancia y la competencia del cuerpo colegido tendría la capacidad de resolver el recurso vertical planteado, cómo segunda instancia y última.

Se propone que su sede será en la ciudad de Quito, en la cual hará oficina el cuerpo colegiado, contando con tres autoridades de protección de datos regionales encontrándose sus oficinas en las ciudades de Guayaquil, Quito y el Tena.

El órgano administrativo, conformado por el pleno que emita resoluciones y actos administrativos, estará conformado por el cuerpo colegiado, teniendo voto dirimente el Superintendente de la agencia. Las Autoridades de Control de Protección del dato, tendrán derecho a participar en las actividades y las sesiones del Consejo, sin derecho a voto.

El pleno de la Agencia de Protección de Datos Ecuatoriana (APDE) será el organismo de jerarquía superior a la Autoridad de Protección de Datos Personales y del Inspector de Protección de Datos.

Los cargos en mención deberán ser ejercidos estrictamente por abogados, especializados en el área de derecho de las TICs o derecho digital.

Misión de la APDE.

La Agencia de Protección de Datos Ecuatoriana (APDE), tiene como objetivo garantizar la aplicación coherente tanto de la Ley cómo el Reglamento General de Protección de Datos Personales y el pleno conformado por el cuerpo colegiado emitirá resoluciones que serán las directrices sobre protección de datos en el ámbito a normarse.

Entre sus atribuciones se encuentra la de adoptar directrices generales para clarificar los términos de la legislación ecuatoriana de protección de datos, proporcionando a todas las partes interesadas una interpretación coherente de sus derechos y obligaciones.

También estarán habilitados para tomar resoluciones vinculantes con respecto a las autoridades nacionales de supervisión para garantizar una aplicación coherente de la normativa, actuando de acuerdo con su reglamento interno y sus principios rectores.

Dentro de sus responsabilidades del Superintendente de Protección de Datos se encuentran las siguientes:

- Proporcionar orientaciones (incluidas directrices, recomendaciones y buenas prácticas) para clarificar la ley.
- Asesorar a la autoridad de protección de datos sobre cualquier aspecto relacionado con la protección de los datos personales y la nueva legislación que se proponga en el país.
- Adoptar políticas públicas para obtener resultados coherentes en casos de transferencias ilegales de datos internacionales.
- Sugerir proyectos de normativa al cuerpo colegiado para la expedición de normas.
- Promover la cooperación y el intercambio efectivo de información y buenas prácticas entre las autoridades nacionales de supervisión y control.
- Elaborar un informe anual de actividades, que sea pública y envía a la Asamblea Nacional, al cuerpo colegiado de la agencia y las demás funciones del Estado.

Los principios rectores que rige al organismo se encuentran lo siguiente:

- **Principio de independencia e imparcialidad.**

La agencia actuará con imparcialidad y con total independencia en el desempeño de sus funciones o el ejercicio de sus competencias.

- **Principios de buena gobernanza, integridad y buena conducta administrativa.**

De conformidad con los principios de buena gobernanza, integridad y buena conducta administrativa, la Agencia actuará en interés público como organismo experto, fiable y autorizado en el ámbito de la protección de datos con buenos procesos de toma de decisiones y buena gestión financiera.

- **Principio de inclusión.**

De conformidad con el principio de inclusión, y con arreglo a las disposiciones de protección de los datos personales utilizados por las autoridades de las diferentes instituciones, la Agencia contará con acuerdos interinstitucionales con las demás Funciones del Estado, con el fin de receptar consideraciones para que sea materia de estudio y desarrollo de normativas en el área tecnológica de los datos.

- **Principio de cooperación.**

De conformidad con el principio de cooperación, la Agencia promoverá la cooperación entre autoridades de control y organismos gubernamentales, se comprometerá a operar siempre que sea posible por consenso.

- **Principio de transparencia.**

De conformidad con el principio de transparencia, la Agencia operará de la manera más abierta posible con el fin de ser más efectivo y más responsable ante las personas.

La Agencia y sus órganos emitirán sus pronunciamientos en un lenguaje claro y comprensible para todos los ciudadanos en idioma español y quichua.

- **Principio de eficiencia y modernización.**

De conformidad con el principio de eficiencia y modernización, la Agencia operará de manera eficiente y con la mayor flexibilidad posible a fin de alcanzar internamente el nivel más elevado de sinergias entre sus departamentos.

El principio de eficiencia y modernización se materializará con el uso de nuevas tecnologías que aporten eficiencia a los métodos de trabajo actuales, como la reducción de las formalidades y el apoyo administrativo eficiente.

- **Principio de proactividad.**

De conformidad con el principio de proactividad, la Agencia anticipará y apoyará por iniciativa propia soluciones innovadoras que ayuden a superar los retos digitales en materia de protección de datos. De esta manera, mediante la participación efectiva de las partes interesadas (miembros, observadores, personal y expertos invitados), se garantizará la plena consideración de las necesidades y aspiraciones de la vida real.

5.5. Resultados Esperados

La propuesta de intervención corresponde a un organismo legítimo que diseñe un sistema de normativas a través del órgano administrativo de la Agencia para proporcionar las garantías necesarias al ciudadano ecuatoriano que, por cualquier situación, pueda sentirse afectado en su derecho a la protección de datos personales.

La Agencia estará capacitada para resolver los requerimientos de los ciudadanos a través de los tres órganos, conforme al trámite que se deba plantear, guía por el órgano administrativo cuyo encargado de elaborar los documentos normativos, los mismos que será las directrices .

Se espera que la Agencia sea una entidad que trabaje en alianza entre lo público y privado, con el fin de procurar beneficios sobre la defensa de los derechos de las personas naturales o jurídicas que puedan estar en perjuicio de protección de sus datos personales y sean susceptible de violaciones de los mismos.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

El entorno legal y operativo en el que se acceden a las TICs dentro de la sociedad ecuatoriana se encuentran regidos por la normativa constitucional y la legislación infra constitucional, normativas jurídicas que no contemplaba una ley de protección de datos personales y con las cuales se limitaba el ejercicio de hacer prevalecer nuestros derechos constitucionales contemplados en la Constitución del Ecuador del 2008, encontrándose vigente cómo la Ley Orgánica de Transparencia y Acceso a la Información Pública, Código de la niñez y adolescencia, Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, Ley de Comercio Electrónico, Firmas y Mensajes de Datos, Código Orgánico Integral Penal (COIP), siendo un gran avance la emisión y publicación en el registro oficial número cuatrocientos cincuenta y nueve, del veintiséis de mayo del dos mil veintiuno, Ley Orgánica de Protección de Datos Personales; la presente ley establece un mecanismo de aplicación, que aunque no tiene la cobertura y de las garantías totales, hace que la situación de la protección de datos personales, pueda llevarse a cabo en un futuro, ya que se otorgó un periodo de dos años para que las empresas públicas, cómo privadas puedan adaptar los procesos conforme la normativa lo establece.

Al realizar la revisión sobre el Derecho y legislación comparada, en cuanto a la normativa vinculada al acceso de datos y posible vulneración de derechos humanos en países de Hispanoamérica, se establece que la Comisión Interamericana de Derechos

Humanos (CIDH) establece que el “internet actualmente constituye una herramienta fundamental de comunicación que permite a las personas vincularse y conectarse de manera ágil, veloz y efectiva, y es considerada una herramienta con un potencial único para el ejercicio de la libertad de expresión”, en este sentido se realizó la revisión de un caso ventilado en la Corte Constitucional de la República de Colombia, quien aborda el derecho a la intimidad, a la honra y al buen nombre en página web o sitio de internet, vulneración efectuada por parte de Google Inc. al haberse negado a eliminar un blog anónimo con contenido difamatorio, deshonoroso y calumnioso contra el demandante y su empresa, el mismo que se pronunció sobre los derechos a la intimidad personal, a la honra y al buen nombre, derecho a la dignidad humana, dejando establecido los límites de la libertad de expresión e información, así como las diferencias entre derecho a la libertad de información y derecho de opinión, delimitando la libertad de expresión en el internet. En este contexto se exhorta al Ministerio de Telecomunicaciones para que establezca una regulación nacional con miras a lograr la protección de los derechos de los usuarios de Internet, especialmente en lo que tiene que ver con publicaciones que atenten contra el honor de las personas en radio, televisión e internet, así como plataformas tecnológicas.

En este caso, Google propició la demanda y la Corte Constitucional de Colombia le otorgó una orden donde se indica que la prohibición de un blog de estas características también constituye una forma de censura que vulnera el derecho a la libertad de expresión y de información.

Al investigar el segundo caso, sobre el pronunciamientos de la Corte Constitucional del Ecuador sobre vulneración de derechos en el ámbito tecnológico, se menciona la acción de protección planteada, en la que se dicta la sentencia, declarando la violación del derecho a la protección de datos personales y autodeterminación informativa, a la imagen y buen nombre e intimidad de la protagonista de fotografías íntimas, al tratar la sentencia de segundo nivel, que resolvió revocar la decisión de primer nivel y declarar sin lugar la acción de habeas data planteado en contra de la persona natural que poseía fotografías íntimas y personales de la actora. Dentro de la sentencia se entra a analizar los conceptos de dato personal, el consentimiento del titular para el

tratamiento de datos personales, el derecho a la intimidad, entre otros derechos conexos al tema.

En cuanto a la propuesta para contribuir a la protección de Datos, que garantice el respeto a la privacidad de las personas, en un entorno justo y equitativo, se llevó a cabo una entrevista a especialistas en el área de estudio y una encuesta ciudadana que permitió establecer el contexto de desarrollo de la propuesta. Entre los principales resultados de la entrevista estuvo que la ciudadanía tiene la percepción que las TICs son un mecanismo por donde se podría ver perjudicados o vulnerados sus derechos (47.9%), donde el principal medio usado son los smartphones (65.4%), que entre las principales redes sociales han identificado a Facebook (76.3%) y WhatsApp (63.8%), consideran además que el uso del Sistema de cámaras de vigilancia de ECU911 puede vulnerar sus derechos (48.7%) y también las empresas tecnológicas que se dedican a recopilar datos o información personal, y al vender la información personal vulneran derechos de los ciudadanos (61.7%).

Al respecto de la entrevista realizada a diversos profesionales, en base al derecho contemplado en el numeral dos del artículo dieciséis de la Constitución del Ecuador; cree usted que su ejercicio tendría como efecto la vulneración de otros derechos de los ciudadanos, contemplados en la Constitución y Tratados Internacionales de Derechos Humanos: la mayoría afirmó que no determinan como una declaración de carácter general que más bien facilita el desarrollo y ejercicio de otros derechos constitucionales, la información personal que decide la persona alimentarla al sistema o plataforma es por cuenta propia ya que el usuario debe manejar de manera responsable dicho acceso. Este es el mecanismo con el que coincidieron la mayoría, de cómo cree usted que las Tecnologías de la Información y Comunicación (TICs), Redes Sociales y aplicaciones tecnológicas, causan o causarían violación de derechos a los usuarios.

La captación indiscriminada por parte de Estados y Empresas tecnológicas, de datos personales de los usuarios de plataformas tecnológicas, expone al ciudadano a que sus datos puedan ser utilizados para desarrollar un control social y/o venta de información con fines similares y de mercado, respecto de los gustos, preferencias de los clientes o usuarios. Siendo un acto abusivo e ilegal el que realizan, por deficiente normativa,

regulaciones de control y sanciones, por ello se plantea la propuesta de la creación de la Agencia de Protección de Datos Ecuatoriana (APDE), con el fin que ejerza control, sanción, así como desarrollo de estudio con el fin de aportar en el área académica y legislativa, para obtener como resultado, normativas jurídicas en defensa del derecho constitucional a la protección de datos de carácter personal.

6.2. Recomendaciones

Se recomienda al Estado, conforme la legislación vigente, implementar políticas públicas, con acuerdos interinstitucionales entre los Ministerio de Educación, el Consejo Nacional de Educación Superior (CONESUP) y Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), actuando cómo ente regulador la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) conforme a sus competencias, en el siguiente punto:

Se impulse programas de educación y capacitación de la ciudadanía en lo que respecta al uso y consumo de las plataformas tecnológicas, redes sociales, así como el desarrollo de conocimiento de sus derechos, protección y defensa de los mismos, con el fin de generar ciudadanos responsables, siendo el efecto la reducción de vulneraciones de derechos constitucionales y reducción del porcentaje de víctimas de ciberdelitos.

Es recomendable en lo que respecta a la Función Ejecutiva, en la red gubernamental de sus instituciones, desarrollo e implementar la utilización de las llamadas firmas sin clave o llave (KSI), utilizando la red blockchain, en temas de gestiones administrativas y en el ámbito de seguridad, con el fin de salvaguardar los derechos de los ciudadanos. Además de ser impulsado su aplicación en el área del sector privado. La cadena de bloques o blockchain, ayudaría a salvaguardar la información y datos personales de los ciudadanos, con el fin de evitar ciberdelitos o violaciones de derechos. Para este propósito se debe de reformar la Ley Orgánica de Protección de Datos en su capítulo sexto, agregando que para la seguridad de datos personales, así como en la aplicación de medidas de seguridad en el ámbito del sector público se debe de aplicar la tecnología blockchain.

Se recomienda el trabajo conjunto de la Función Judicial, con la Función Legislativa en la creación de políticas públicas, desarrollo, emisión y reforma de leyes,

para que el ciberespacio sea un lugar seguro para los usuarios, respetando los derechos humanos, actualizando las normativas conforme el desarrollo de la tecnología.

En lo que respecta a la competencia de la Asamblea Nacional del Ecuador, se recomienda reformar la Ley Orgánica de Protección de Datos, con el fin de que se agregue el derecho al olvido, derecho que no fue contemplado en la ley.

Así mismo, se recomienda a la Asamblea Nacional del Ecuador expedir el Reglamento de la Ley Orgánica de Protección de Datos, con el fin que conste las directrices, requisitos y procedimientos sobre el control que se debe realizar a las entidades que usan datos personales para su tratamiento, las que deberán justificar cuales son los datos que tratan, el uso que los dan, así como su propósito, además de la información sobre las transferencias que realizan a países extranjeros, con el fin de proteger los derechos de los ciudadanos.

En la recomendación de reforma a la Ley Orgánica de Protección de Datos y en la expedición de su Reglamento debe de tratarse sobre la aplicación de las cookies en páginas web, tanto de las plataformas gubernamentales como particular, las mismas que debe de contener la opción de aceptar o declinar para que el usuario elija si desea o no, que sus datos sean captados o tratados, ya que por la simple navegación en una página web no expresa consentimiento, además en el desarrollo de los muros de cookies deben de contener obligatoriamente alternativas que equivalente a aceptar o declinar si otorga el consentimiento, caso contrario deben ser prohibidas.

Se recomienda la reforma de la Ley Orgánica de Protección de Datos Personales, en el sentido que se prohíba la transferencia de datos de los ciudadanos ecuatorianos a un país extranjero o de origen de la compañía o plataforma tecnológica, así como el cruce de datos entre plataformas de redes sociales que pertenezcan a una misma compañía, con el fin de evitar vulneración de derechos.

Así mismo es recomendable que conste en la Ley Orgánica de Protección de Datos Personales, que las compañías tecnológicas que presten servicio con sus plataformas tecnológicas y de tratamiento de datos, necesariamente se encuentren domiciliadas en el país, para que se responsabilicen sobre su accionar y sean parte

procesal en acciones legales. Entre ellas Google, Meta Platforms, Inc. (anteriormente conocida como Facebook, Inc) y Twitter, Inc.

Además, se recomienda la reforma de la Ley Orgánica de Protección de Datos Personales, con el fin de crear la Agencia de Protección de Datos Ecuatoriana (**APDE**), conforme los parámetros establecidos en el capítulo cinco.

Se recomienda derogar el Acuerdo Ministerial 012-2019, expedido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información, el mismo que determina la política de tratamiento de datos personales, el mismo que viola derechos, por cuando obliga a aceptar los términos y condiciones, no siendo consentido de forma voluntaria.

Se recomienda a la ciudadanía actuar de forma responsable en lo que corresponde al uso de la tecnología, por las controversias generadas a nivel mundial, por las cuales llegamos a dudar de la fiabilidad de las plataformas tecnológicas, por ende, se insta a compartir menos datos personales o información personal en plataformas de redes sociales y correo electrónico, así mismo configurar las opciones, eliminando que los datos se guarden en la nube, además de mantener la seguridad contra terceras personas.

Recomiendo utilizar la tecnológica para lo estrictamente necesario, ya que, si la utilizamos de una manera despreocupada, podríamos ser además víctimas de delitos y ciberdelitos.

6.3. Limitaciones

La situación del país actualmente, puede perjudicar el desarrollo de la propuesta en cuanto a la priorización del tema a ser atendido. Además de la disposición de la Autoridad de protección de datos para llevar adelante lo correspondiente.

La suma de esfuerzo entre el sector público y privado puede llevar más tiempo del que se plantea. Debido a esto, las ideas y consensos pueden quedar diluidas. La discusión debe llevarse a niveles de Asamblea y lograr que la mayor cantidad de actores se sumen a esta propuesta.

CAPITULO VII

REFERENCIAS BIBLIOGRÁFICAS

- akus.net. (08 de Junio de 2021). *Internet ¿Qué es? Definición y Significado*. (H. Delgado, Editor)
Recuperado el 12 de Agosto de 2021, de <https://disenowebakus.net/internet.php>
- Almada Torres, F. (3 de Junio de 2020). *Círculo de análisis Euromediterráneo*. Recuperado el 30 de 03 de 2021, de <http://circuloeuromediterraneo.org/dictaduras-digitales/>
- Álvarez, J., Camacho, M., & Maldonado, G. (2020). *La investigación cualitativa*. Obtenido de <https://www.uaeh.edu.mx/scige/boletin/tlahuelilpan/n3/e2.html>.
- Annan, K. (Febrero de 2018). *Nueva Sociedad*. Obtenido de <https://nuso.org/articulo/como-las-tecnologias-de-la-informacion-amenazan-la-democracia-annan-nuso/>
- Arias, F. (2014). *El Proyecto de Investigación*. Obtenido de <https://evidencia.com/wp-content/uploads/2014/12/EL-PROYECTO-DE-INVESTIGACION-C3%93N-6ta-Ed.-FIDIAS-G.-ARIAS.pdf>.
- Asamblea Nacional del Ecuador. (20 de Octubre de 2008). Constitución de la República del Ecuador. Ecuador: Registro Oficial del Ecuador. Recuperado el 17 de Agosto de 2021, de <https://www.fielweb.com/Index.aspx?157Rabf6ik65998>
- Barranco Fragoso, R. (18 de Junio de 2012). *IBM Developer*. Recuperado el 12 de Agosto de 2021, de <https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/index.html>
- Bauman, Z., & Lyon, D. (2013). *Vigilancia líquida* (Primera ed.). Paidós. Recuperado el 14 de Junio de 2021
- BBC NEWS. (20 de Junio de 2018). *BBC News Mundo*. Recuperado el 2021 de Agosto de 2021, de <https://www.bbc.com/mundo/noticias-44496050>
- Bernal Pulido, C. (2018). *Derechos, cambios constitucional y teoría jurídica*. (Primera ed.). Universidad externado de Colombia. Recuperado el 14 de Junio de 2021
- Bernal, C. (2010). *Metodología de la investigación*. (Tercera ed.). Pearson. Recuperado el 14 de Junio de 2021

- Carbonell, M. (2007). *Teoría del neoconstitucionalismo. Ensayos escogidos*. Trotta, S.A.
Recuperado el 22 de Junio de 2021
- Carbonell, M. (2009). *Neoconstitucionalismo (s)* (Cuarta ed.). (M. Carbonell, Ed.) Trotta.
Recuperado el 22 de Junio de 2021
- Carbonell, M., & Salazar, P. (s.f.). *Garantismo. Estudio sobre el pensamiento jurídico de Luigi Ferrajoli* (Segunda ed.). (M. Carbonell, & P. Salazar, Edits.) Trotta. Recuperado el 22 de Junio de 2021
- Clinic Cloud. (24 de Marzo de 2019). *Clinic Cloud*. (F. Llordachs Marqués, Editor) Recuperado el 17 de Agosto de 2021, de <https://clinic-cloud.com/blog/beneficios-tics-en-salud/>
- Comisión Europea. (Julio de 2016). *Comisión Europea*. Recuperado el 12 de Agosto de 2021, de https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_es
- Concepto. (2020). *¿Qué es la Fenomenología?* Obtenido de <https://concepto.de/fenomenologia/>.
- Corte Constitucional del Ecuador. (14 de Septiembre de 2015). *Corte Constitucional del Ecuador*. Recuperado el 18 de Agosto de 2021, de <http://doc0.corteconstitucional.gob.ec:8080/alfresco/d/d/workspace/SpacesStore/89e18c1f-7f1f-4648-b1b2-17b446a58aaf/1493-10-EP-sen.pdf?guest=true>
- Corte Constitucional del Ecuador. (01 de Julio de 2020). *Corte Constitucional del Ecuador*. Obtenido de https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiptJnL2LryAhWMRTABHQb0DbgQFnoECCUQAQ&url=https%3A%2F%2Fwww.funcionjudicial.gob.ec%2Fwww%2Fpdf%2FSentencia%2520No%25205-14-JD20.pdf&usg=AOvVaw3Bxe_RaN0qCVcST5Qma6Th
- Corte Constitucional del Ecuador. (27 de Enero de 2021). *Corte Constitucional del Ecuador*. Recuperado el 18 de Agosto de 2021, de <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjsj4qlganyAhWgkWoFHQICBu04ChAWegQIAxAB&url=https%3A>

%2F%2Fwww.funcionjudicial.gob.ec%2Fwww%2Fpdf%2FSentencia%25C2%25A0206
4-14-EP21.pdf&usg=AOvVaw0wze7ZoSkhfHqUZ5SY6sOU

Corte Constitucional República de Colombia. (09 de Mayo de 2018). *Corte Constitucional República de Colombia*. Recuperado el 18 de Agosto de 2021, de <https://www.corteconstitucional.gov.co/relatoria/2017/t-063a-17.htm>

Dasandi, N., & Taylor, M. (2019). *Falla la democracia?* Blume.

de la Iglesia Prado, E. (2018). *Derecho digital: Retos y cuestiones actuales* (Primera ed., Vol. 16). Aranzandi, S.A.U. Recuperado el 14 de Junio de 2021

Dejusticia. (12 de Febrero de 2020). *Dejusticia*. (D. Ospina Celis, Editor) Recuperado el 17 de Agosto de 2021, de <https://www.dejusticia.org/column/como-las-empresas-recolectan-tus-datos/>

Diccionario de la lengua española. (Diciembre de 2019). *Real Academia Española*. Recuperado el 12 de Agosto de 2021, de <https://dle.rae.es/?w=tecnolog%C3%ADa>

DW Akademie. (Abril de 2016). (D. Akademie, Ed.) Recuperado el 21 de Mayo de 2021, de https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjbg9eNgdzwAhU1ITQIHe2_Az4QFjAAegQIBBAD&url=https%3A%2F%2Fwww.dw.com%2Fdownloads%2F30336831%2Fpanorama-de-los-medios-en-ecuador-pdf.pdf&usg=AOvVaw0NLIWJ66C3KcvQTSbeHb

DW Español. (27 de Mayo de 2021). WhatsApp y sus alternativas. Youtube. Recuperado el 17 de Agosto de 2021, de <https://www.youtube.com/watch?v=AoYrF7ciBj8>

Ecured. (2020). *Investigación social*. Obtenido de https://www.ecured.cu/Investigaci%C3%B3n_social.

Educación. (2020). *Qué es la investigación de campo — Etapas, características y técnicas*. Obtenido de <https://www.recursosdeautoayuda.com/investigacion-de-campo/>.

Estados Americanos. (22 de Noviembre de 1969). Convención Americana sobre Derechos Humanos "Pacto de San José de Costa Rica". Recuperado el 17 de Agosto de 2021, de <https://www.fielweb.com/Index.aspx?157Rabf6ik65998#app/buscador>

- Fernández Delpech, H. (2014). *Manual de derecho informático* (Primera ed.). Abeledoperrot. Recuperado el 14 de Junio de 2021
- FERNANDEZ, E. J. (2014). *La proteccion y seguridad de la persona en internet. Aspectos osciales y juridicos*. (R. Calvo, Ed.) Madrid: Editorial Reus, S.A. Recuperado el 27 de Junio de 2021
- Fisterra. (2020). *Investigación cuantitativa y cualitativa*. Obtenido de <https://www.fisterra.com/formacion/metodologia-investigacion/investigacion-cuantitativa-cualitativa/>.
- France 24 Español. (8 de Mayo de 2019). *France 24 Español*. Obtenido de https://www.youtube.com/watch?v=pZu9N-3yn_M
- Global Freedom of Expression Columbia University. (03 de Marzo de 2021). *Global Freedom of Expression Columbia University*. Recuperado el 18 de Agosto de 2021, de <https://globalfreedomofexpression.columbia.edu/cases/fierro-v-google-inc-2/?lang=es>
- Gutiérrez-Rubí, A. (2015). *La política en tiempos de WhatsApp*. EL PAÍS. Recuperado el 12 de Agosto de 2021, de <https://play.google.com/books/reader?id=Obi3BwAAQBAJ&pg=GBS.PT1>
- Hernandez, Sampieri, & Baptista. (2019). *Metodología de la investigación*. Obtenido de https://www.esup.edu.pe/descargas/dep_investigacion/Metodologia%20de%20la%20investigacion%20de%20Edici%C3%B3n.pdf.
- Jimenez, R. (1998). *Estudios descriptivos*. . Obtenido de http://www.sld.cu/galerias/pdf/sitios/bioestadistica/metodologia_de_la_investigacion_1998.pdf.
- La Comisión Federal de Comercio. Información para consumidores. (Septiembre de 2011). *La Comisión Federal de Comercio. Información para consumidores*. Recuperado el 12 de Agosto de 2021, de <https://www.consumidor.ftc.gov/articulos/s0018-aplicaciones-moviles-que-son-y-como-funcionan>
- Matos, A. (2020). *Investigación Bibliográfica: Definición, Tipos, Técnicas*. Obtenido de <https://www.lifeder.com/investigacion->

bibliografica/#:~:text=La%20investigaci%C3%B3n%20bibliogr%C3%A1fica%20o%20documental,selecci%C3%B3n%20de%20fuentes%20de%20informaci%C3%B3n.

Mozur, P., Kessel, J., & Chan, M. (24 de Abril de 2019). Hecho en China y exportado a Ecuador: el aparato de vigilancia estatal. *Hecho en China y exportado a Ecuador: el aparato de vigilancia estatal*. Obtenido de <https://www.nytimes.com/es/2019/04/24/espanol/america-latina/ecuador-vigilancia-seguridad-china.html>

Murga Fernández, J. (2018). *Derecho Digital: Retos y cuestiones actuales*. España: Aranzadi, S.A.U. Recuperado el 17 de Agosto de 2021

Naciones Unidas. (10 de Diciembre de 1948). *Organización de las Naciones Unidas*. Obtenido de https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwisp7bo4rnyAhU2TjABHVgHC08QFnoECAMQAQ&url=https%3A%2F%2Fwww.un.org%2Fes%2Fdocuments%2Fudhr%2FUDHR_booklet_SP_web.pdf&usg=AOvVaw2A18iou2nCX9HHSPURd6g1

Naciones Unidas. (27 de Junio de 2016). *Naciones Unidas. Derechos Humanos. Oficina del alto Comisionado*. Recuperado el 12 de Agosto de 2021, de https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_32_L20.pdf

Naciones Unidas. (s.f.). *Naciones Unidas*. Recuperado el 22 de Junio de 2021, de <https://www.un.org/es/global-issues/human-rights>

OEA. (Agosto de 2009). *Organización de los Estados Americanos (OEA)*. Recuperado el 12 de Agosto de 2021, de http://www.oas.org/es/temas/sociedad_conocimiento.asp

OEA. (16 de Agosto de 2021). *OEA*. Recuperado el 18 de Agosto de 2021, de <http://www.oas.org/es/cidh/mandato/que.asp>

Parlamento Europeo. (26 de Marzo de 2021). *Noticias Parlamento Europeo*. Recuperado el 12 de Agosto de 2021, de <https://www.europarl.europa.eu/news/es/headlines/society/20200827STO85804/que-es-la-inteligencia-artificial-y-como-se-usa>

- Parlamento Europeo, el Consejo y la Comisión. (26 de Octubre de 2012). *Comisión Europea*. Recuperado el 17 de Agosto de 2021, de <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12012P/TXT&from=ES>
- Pérez Porto , J., & Merino, M. (2014). *DEFINICIÓN DE*. Recuperado el 12 de Agosto de 2021, de <https://definicion.de/smartphone/>
- Psyma. (2015). *¿Cómo determinar el tamaño de una muestra?* Obtenido de <https://www.psyma.com/company/news/message/como-determinar-el-tamano-de-una-muestra>.
- QuestionPro. (2020). *¿Qué es la Investigación Exploratoria?* Obtenido de <https://www.questionpro.com/blog/es/investigacion-exploratoria/>.
- RAE; Real Academia Española. (2020). *Diccionario panhispánico del español jurídico*. Recuperado el 12 de Agosto de 2021, de <https://dpej.rae.es/lema/red-social>
- Ramírez, T. (2010). *Cómo hacer un proyecto de investigación*.
- Raul, E. (2009). *Técnicas de Investigación de Campo*. Obtenido de <http://niveldostic.blogspot.com/2009/06/metodo-analitico-sintetico.html>.
- Real Academia Española. (2005). *Diccionario panhispánico de dudas*. Recuperado el 12 de Agosto de 2021, de <https://www.rae.es/dpd/computador>
- Real Academia Española. (13 de Enero de 2018). *Real Academia Española*. Recuperado el 12 de Agosto de 2021, de <https://dle.rae.es/internet>
- Real Academia Española. (2020). *Diccionario panhispánico del español jurídico*. Recuperado el 12 de Agosto de 2021, de <https://dpej.rae.es/lema/videoc%C3%A1mara-en-lugar-p%C3%ABlico>
- Real Academia Española. (10 de Diciembre de 2020). *Diccionario panhispánico del español jurídico*. Recuperado el 12 de Agosto de 2021, de <https://dpej.rae.es/lema/derechos-humanos>
- Real Academia Española. (2020). *Diccionario panhispánico del español jurídico*. Recuperado el 12 de Agosto de 2021, de <https://dpej.rae.es/lema/derecho-fundamental>

- Real Academia Española. (2020). *Real Academia Española*. Recuperado el 12 de Agosto de 2021, de <https://dle.rae.es/videovigilancia>
- Real Academia Española. (9 de Junio de 2020). *Real Academia Española*. Recuperado el 12 de Agosto de 2021, de <https://dle.rae.es/tel%C3%A9fono?m=form#GkqQMnE>
- Rodriguez, A. (2020). *Método analítico de investigación: características y ejemplos*. Obtenido de <https://www.lifeder.com/metodo-analitico-sintetico/>.
- Schwab, K. (2016). *La cuarta revolución industrial*. DEBATE. Recuperado el 11 de Agosto de 2021, de <https://play.google.com/books/reader?id=BRonDQAAQBAJ&pg=GBS.PP1>
- Servicio Integrado de Seguridad Ecu911. (03 de Septiembre de 2017). *Servicio Integrado de Seguridad Ecu911*. Recuperado el 12 de Agosto de 2021, de <https://www.ecu911.gob.ec/camaras-de-videovigilancia/>
- Simeon, P. (s.f.). <https://www.psyma.com/company/news/message/como-determinar-el-tamano-de-una-muestra>.
- Softonic. (04 de Agosto de 2014). *Softonic*. (S. Marc, Editor) Recuperado el 17 de Agosto de 2021, de <https://www.softonic.com/articulos/6-terminos-y-condiciones-que-aceptas-sin-saber>
- Sosa, J. N. (s.f.). *Big Data Comunicacion y Politica* . Teatro de Ediciones.
- Telefónica. (20 de Enero de 2021). *Telefónica*. Obtenido de <https://www.telefonica.com/es/web/negocio-responsable/articulo/-/blogs/-que-ventajas-ofrecen-las-tic-a-las-pymes->
- UNAM. (2018). *Investigación bibliográfica* . Obtenido de <http://paginas.facmed.unam.mx/deptos/ss/wp-content/uploads/2018/10/12.pdf>.
- UNIR. (16 de Mayo de 2021). *UNIR la universidad en internet*. Recuperado el 17 de Agosto de 2021, de <https://www.unir.net/educacion/revista/tic-en-el-aula/>
- USON. (2018). *MUESTREO*. Obtenido de <http://www.estadistica.mat.uson.mx/Material/elmuestreo.pdf>.

Wylie, C. (19 de 03 de 2020). *Mindf*ck. Cambridge analytica la tramapara desestabilizar el mundo*. Editorial Roca.

VIII

APÉNDICE

Anexo I. Encuesta de opinión para la ciudadanía

ENCUESTA PARA DETERMINAR SI EL ACCESO A LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TICS) COMO DERECHO ESTABLECIDO EN LA CONSTITUCIÓN DEL ECUADOR DE 2008 Y SU EFECTO SISTEMÁTICO DE VULNERACIÓN DE DERECHOS DE LOS CIUDADANOS.

Agradecemos su participación en esta encuesta que tiene la finalidad de conocer la opinión de la ciudadanía ecuatoriana en lo que respecta a la conciencia que tiene sobre la protección de sus datos, así como sus derechos, al momento de utilizar las TICs y Redes Sociales. Los datos serán utilizados con fines académicos para la investigación que se titula: “El acceso a las tecnologías de la información y comunicación (TICs) como derecho establecido en la constitución del Ecuador de 2008 y su efecto sistemático de vulneración de derechos de los ciudadanos.

Toda la información que usted nos facilite permanecerá en total confidencial y anonimato. Por tal motivo y agradeciéndole con su participación y colaboración ponemos a consideración el siguiente cuestionario. Si tiene alguna duda con respecto a las preguntas, por favor solicitar una aclaración de las mismas con el encuestador.

Atte.:

Abg. Omar Altamirano Villena.

MAESTRANTE EN DERECHO CONSTITUCIONAL.

Encuesta elaborada desde julio del 2021.

Datos socio-demográficos

1.- Rango de edad:

GZ 16-20 años **GY 21-40 años** **GX41-55 años** **G BB 56-74 años**

2.- Sexo: Masculino Femenino

3.- Instrucción Educativa:

Primaria Secundaria Tercer Nivel Post Grado Ninguna de las anteriores

4.- Usted cree que con el acceso a las Tecnologías de la Información y Comunicación (TICs) se podrían ver perjudicados o vulnerados sus derechos?

Totalmente de acuerdo

Medianamente de acuerdo

Estoy de Acuerdo

Medianamente en desacuerdo

Totalmente en desacuerdo

No tengo conocimiento

5.- Si la respuesta fue afirmativa en la pregunta anterior. ¿Cuales derechos cree usted se verían perjudicados o vulnerados por el uso de las TICs? (Señale una o más opciones)

Derecho a la protección de datos de carácter personal

Derecho a la inviolabilidad y al secreto de la correspondencia física y virtual

Derecho a la libertad de expresión

Derecho a la libertad de información

Derecho a la intimidad personal y familiar

Derecho al honor y buen nombre

Derecho a la imagen

Derecho a la protesta

Derecho a la libertad de tránsito y libre movilidad

Ninguno de los anteriores

No tengo conocimiento

6.- ¿ Con que Tecnología de la Información y Comunicación (TICs) usted cree que se podrían vulnerar los derechos antes señalados? (Señale una o más opciones)

Radio Teléfono convencional Televisor Celular básico, solo llamadas
 Celular Inteligente (Smartphone) Internet Computadoras Ninguna de las anteriores No tengo conocimiento

Otro (Especifique): _____

7.- ¿Usted cree que con el uso de las redes sociales se podría ver perjudicados o vulnerados sus derechos?

Totalmente de acuerdo

Medianamente de acuerdo

Estoy de Acuerdo

Medianamente en desacuerdo

Totalmente en desacuerdo

No tengo conocimiento

8.- ¿ Con que redes sociales usted cree que se podrían vulnerar los derechos antes señalados? (Señale una o más opciones)

Facebook WhatsApp Twitter YouTube Snapchat Instagram

Tik Tok LinkedIn Telegram Facebook Messenger Spotify Ninguna

Otra (Especifique): _____

9.- ¿Usted cree que el sistema de cámaras de vigilancia instalado por el Ecu911 puede limitar o vulnerar derechos?

Totalmente de acuerdo

Medianamente de acuerdo

Estoy de Acuerdo

Medianamente en desacuerdo

Totalmente en desacuerdo

No tengo conocimiento

10.- Si respondi si en la pregunta anterior. ¿Cuáles derechos cree usted que restringirían o vulnerarían. (Señale una o más opciones)

Derecho a la protección de datos de carácter personal

Derecho a la inviolabilidad y al secreto de la correspondencia física y virtual

Derecho a la libertad de expresión

Derecho a la libertad de información

Derecho a la intimidad personal y familiar

Derecho al honor y buen nombre

Derecho a la imagen

Derecho a la protesta

Derecho a la libertad de tránsito y libre movilidad

Ninguno de los anteriores

No tengo conocimiento

11.- ¿Usted cree que las empresas y/o el Estado al recopilar datos o información de personas en la web, dispositivos electrónicos y de vigilancia, vulneran o vulnerarían derechos de los ciudadanos?

Totalmente de acuerdo

Medianamente de acuerdo

Estoy de Acuerdo

Medianamente en desacuerdo

Totalmente en desacuerdo

No tengo conocimiento

12.- Si respondió si en la pregunta anterior. ¿Cuáles derechos de los ciudadanos cree usted que se restringirían o vulnerarían. (Señale una o más opciones)

Derecho a la protección de datos de carácter personal

Derecho a la inviolabilidad y al secreto de la correspondencia física y virtual

Derecho a la libertad de expresión

Derecho a la libertad de información

Derecho a la intimidad personal y familiar

Derecho al honor y buen nombre

Derecho a la imagen

Derecho a la protesta

Derecho a la libertad de tránsito y libre movilidad

Ninguno de los anteriores

No tengo conocimiento

13.- ¿Usted cree que las empresas que se dedican a recopilar datos o información personal, al venderlas vulneran derechos de los ciudadanos?

Totalmente de acuerdo

Medianamente de acuerdo

Estoy de Acuerdo

Medianamente en desacuerdo

Totalmente en desacuerdo

No tengo conocimiento

14.- Si respondió si en la pregunta anterior. ¿Cuales derechos de los ciudadanos cree usted que se restringirían o vulnerarían? (Señale una o más opciones)

Derecho a la protección de datos de carácter personal

Derecho a la inviolabilidad y al secreto de la correspondencia física y virtual

Derecho a la libertad de expresión

Derecho a la libertad de información

Derecho a la intimidad personal y familiar

Derecho al honor y buen nombre

Derecho a la imagen

Derecho a la protesta

Derecho a la libertad de tránsito y libre movilidad

Ninguno de los anteriores

No tengo conocimiento

15.- ¿Usted considera que, con el avance de la tecnología, deberíamos tener derecho a decidir qué uso se da a nuestra información personal?

Totalmente de acuerdo

Medianamente de acuerdo

Estoy de Acuerdo

Medianamente en desacuerdo

Totalmente en desacuerdo

No tengo conocimiento

16.- ¿Usted cree que debería de existir un derecho en el que toda la información que usted haya generado o compartido sea eliminada de las bases de datos, tanto privados como gubernamentales?

Totalmente de acuerdo

Medianamente de acuerdo

Estoy de Acuerdo

Medianamente en desacuerdo

Totalmente en desacuerdo

No tengo conocimiento

17.- ¿Usted considera que, con el avance de la tecnología, deberíamos tener derecho a decidir qué uso se da a nuestra información personal?

Totalmente de acuerdo

Medianamente de acuerdo

Estoy de Acuerdo

Medianamente en desacuerdo

Totalmente en desacuerdo

No tengo conocimiento

18.- En una escala del 1 al 10 siendo el 1 lo más bajo y 10 lo más alto, que tan capacitadas cree que se encuentran las instituciones públicas del Ecuador para evitar el robo de datos y reaccionar exitosamente para solucionar el problema y proteger la información de sus ciudadanos?

1 2 3 4 5 6 7 8 9 10

No tengo conocimiento

19.- ¿Cree usted que la Asamblea Nacional debe preocuparse de legislar en el área tecnológica que involucre al ser humano, entre ello, del tratamiento de datos personales y seguridad de su información personal?

Totalmente de acuerdo

Medianamente de acuerdo

Estoy de Acuerdo

Medianamente en desacuerdo

Totalmente en desacuerdo

No tengo conocimiento

384 respuestas



No se aceptan más respuestas



Mensaje para los encuestados

Ya no se aceptan respuestas en este formulario

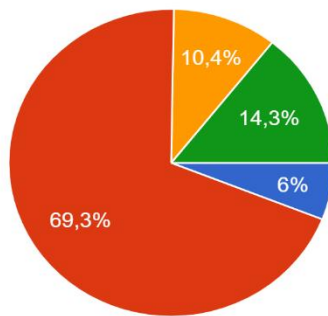
Resumen

Pregunta

Individual

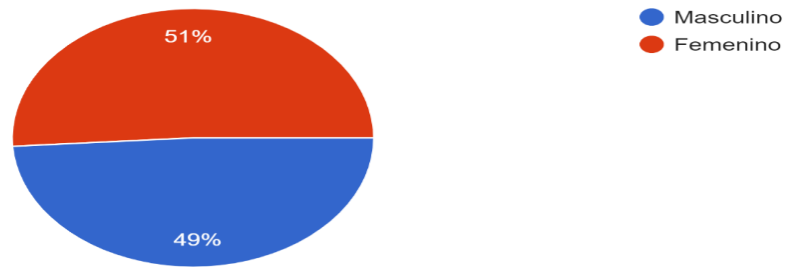
1.- Rango de edad:

384 respuestas

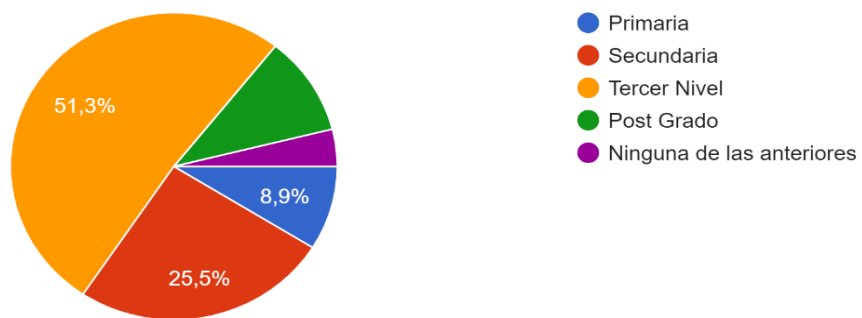


- GZ 16-20 años
- GY 21-40 años
- GX41-55 años
- G BB 56-74 años

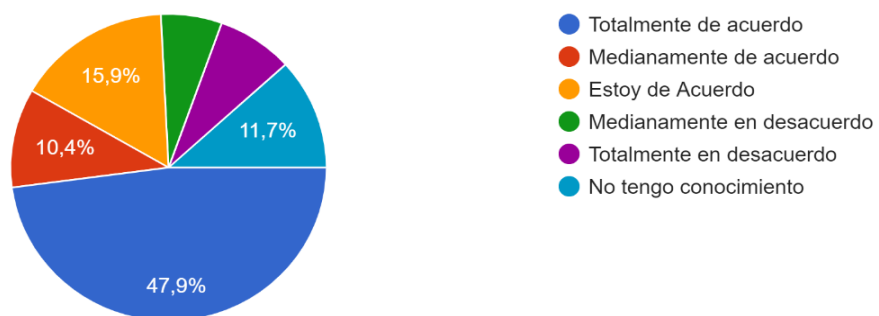
2.- Sexo:
384 respuestas



3.- Instrucción Educativa:
384 respuestas

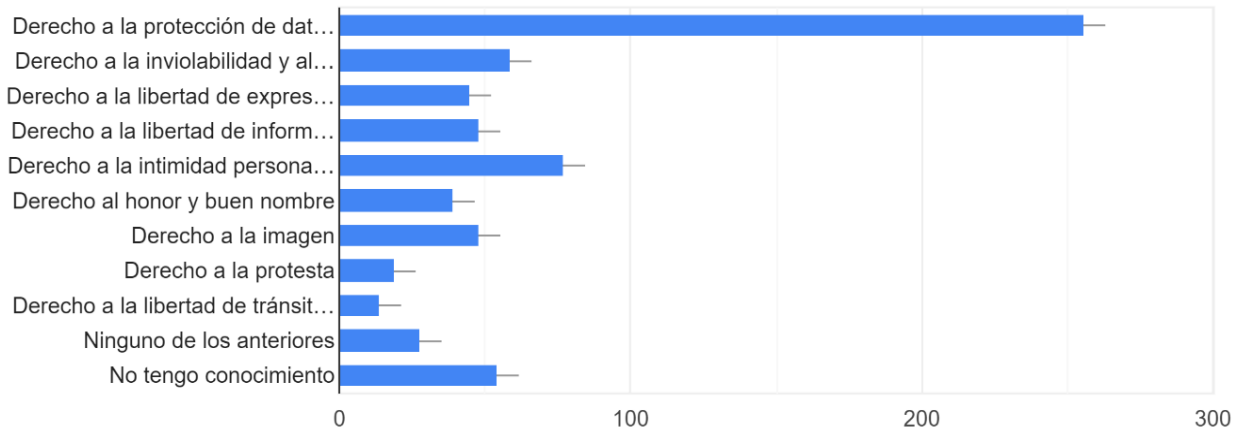


4.- ¿Usted cree que con el acceso a las Tecnologías de la Información y Comunicación (TICs) se podrían ver perjudicados o vulnerados sus derechos?
384 respuestas



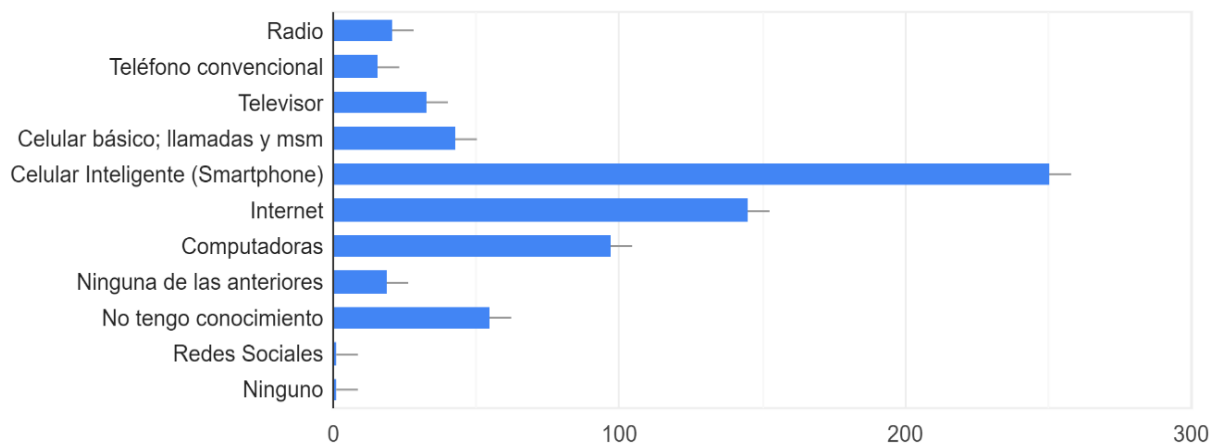
5.- Si la respuesta fue afirmativa en la pregunta anterior. ¿Cuáles derechos cree usted que se verían perjudicados o vulnerados por el uso de las TICs? (Señale una o más opciones).

384 respuestas



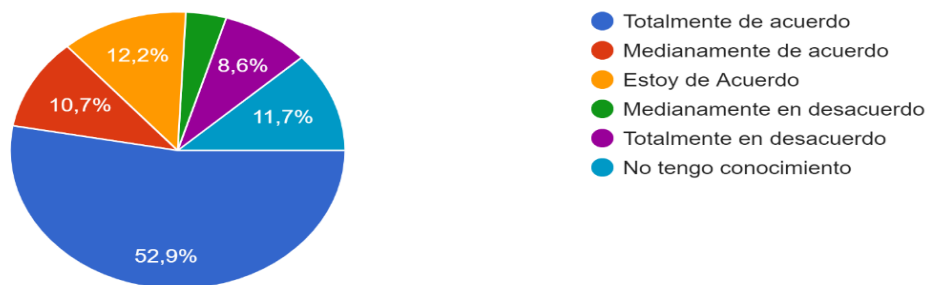
6.- ¿Con que Tecnología de Información y Comunicación (TICs) usted cree que se podrían vulnerar los derechos antes señalados? (Señale una o más opciones).

384 respuestas



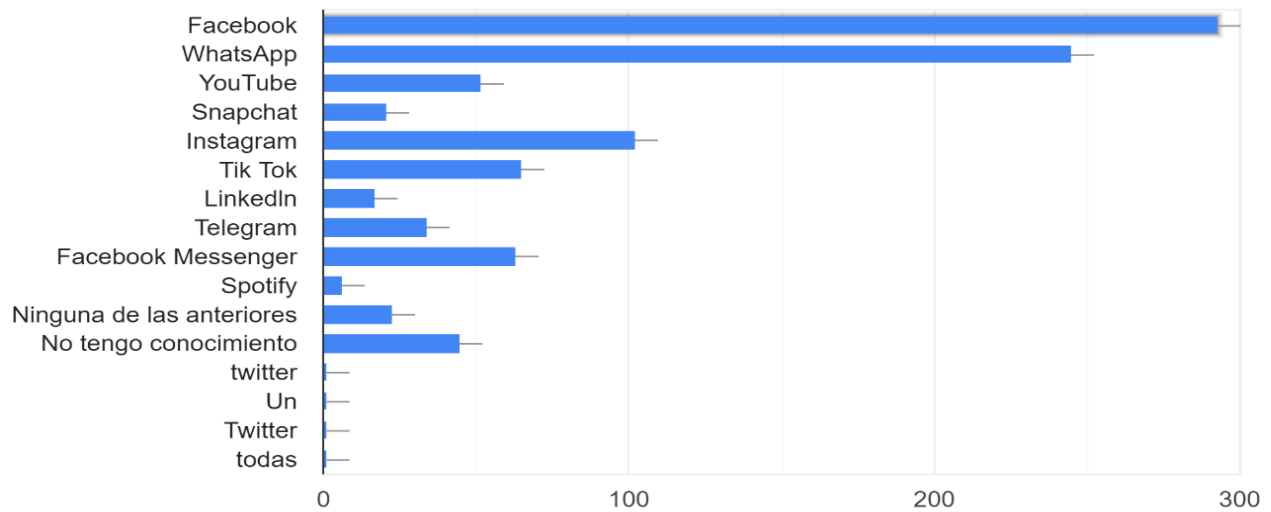
7.- ¿Usted cree que con el uso de las redes sociales se podrían ver perjudicados o vulnerados sus derechos?

384 respuestas



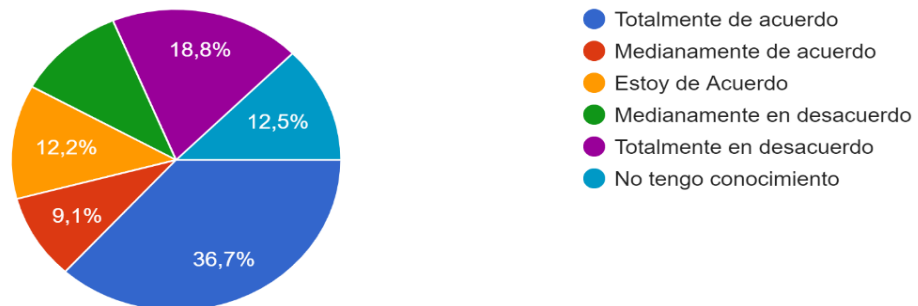
8.- ¿ Con que redes sociales usted cree que se podrían vulnerar los derechos antes señalados?
(Señale una o más opciones).

384 respuestas



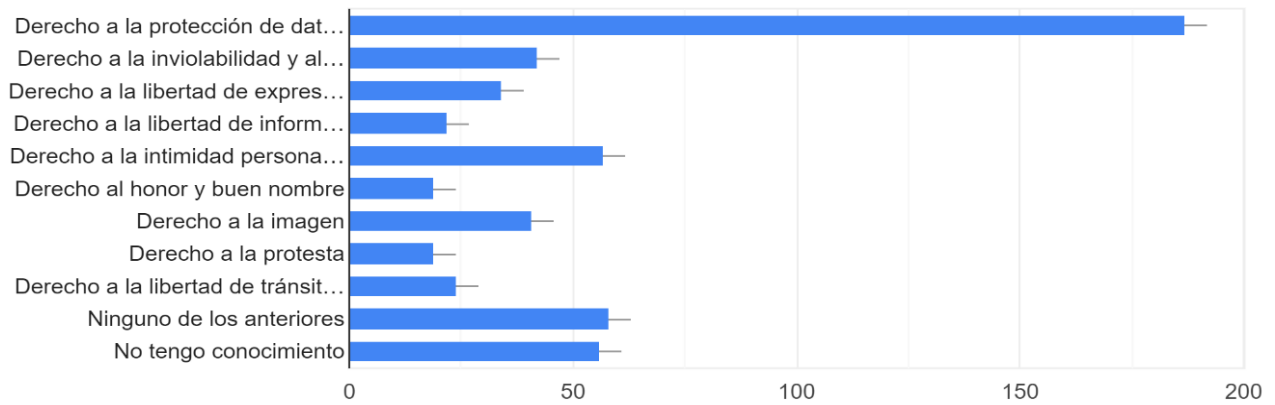
9.- ¿Usted cree que el sistema de cámaras de vigilancia instalado por el Ecu911, puede limitar o vulnerar derechos?

384 respuestas



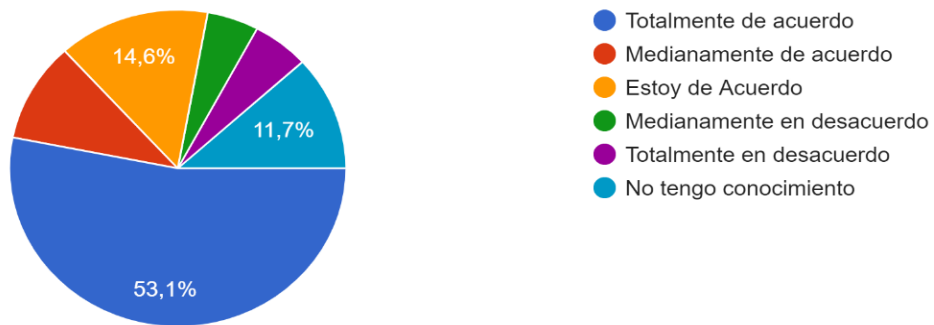
10.- Si respondió si en la pregunta anterior. ¿Cuáles derechos cree usted que se restringirían o vulnerarían? (Señale una o más opciones).

384 respuestas



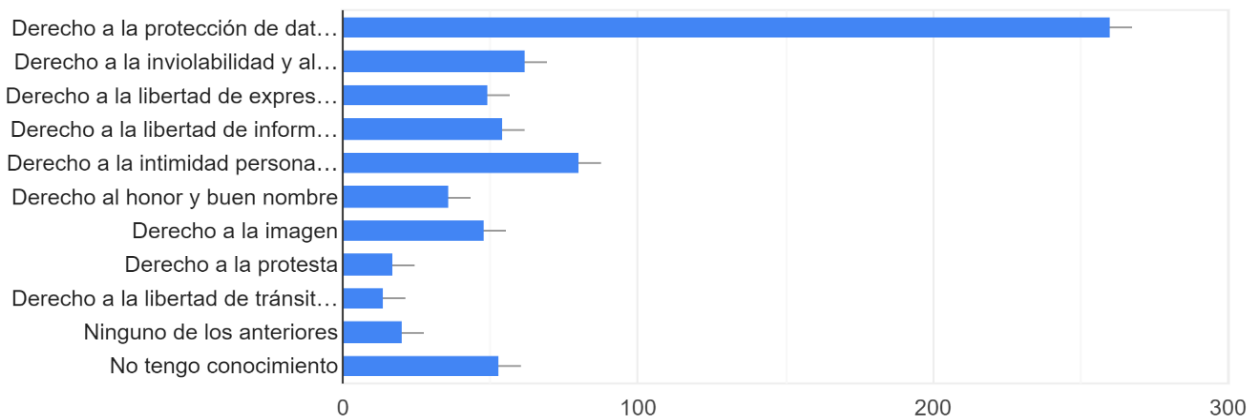
11.- ¿Usted cree que las empresas y/o el Estado, al recopilar datos o información de personas en la web, dispositivos electrónicos y de vigilancia, vulneran o vulnerarían derechos de los ciudadanos?

384 respuestas



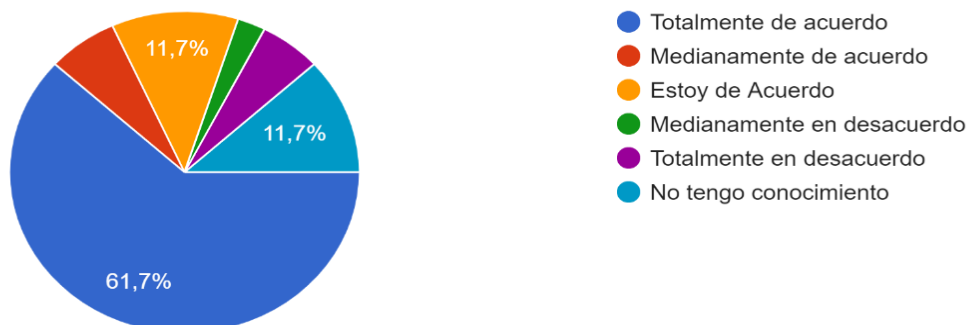
12.- Si respondió si en la pregunta anterior. ¿Cuáles derechos de los ciudadanos cree usted que se restringirían o vulnerarían? (Señale una o más opciones).

384 respuestas



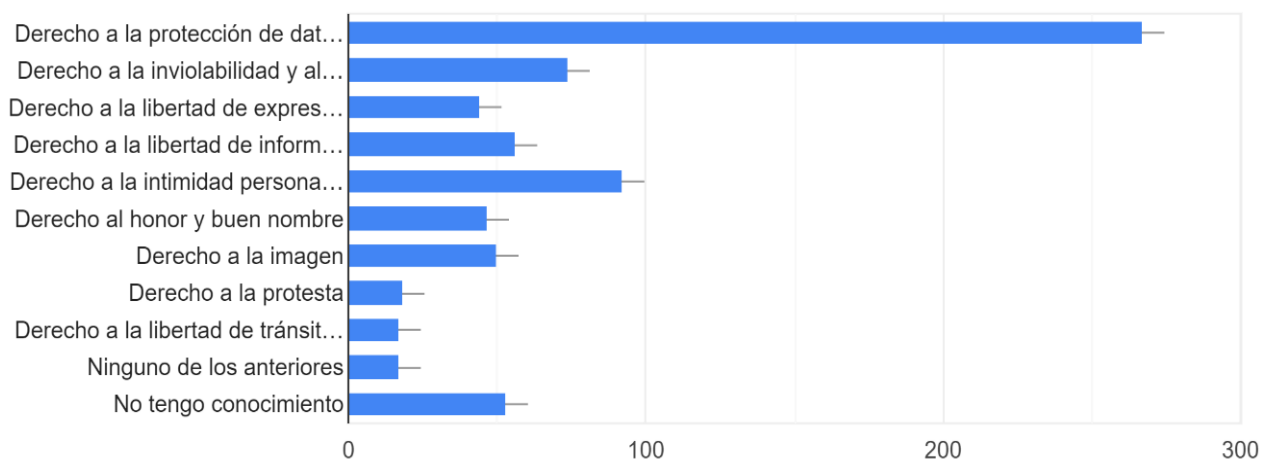
13.- ¿Usted cree que las empresas que se dedican a recopilar datos o información personal, al venderlas vulneran derechos de los ciudadanos?

384 respuestas



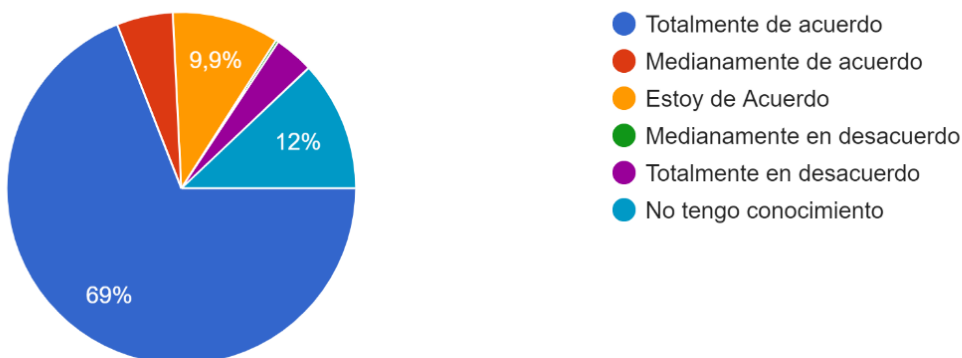
14.- Si respondió si en la pregunta anterior. ¿Cuáles derechos de los ciudadanos cree usted que se restringirían o vulnerarían? (Señale una o más opciones).

384 respuestas



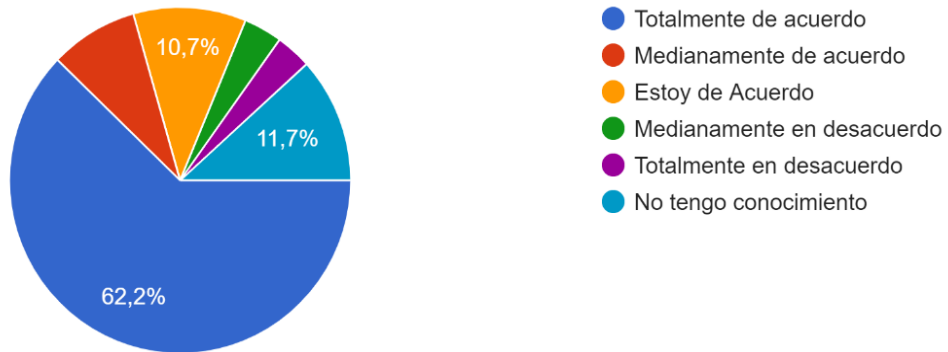
15.- ¿Usted considera que, con el avance de la tecnología, deberíamos tener derecho a decidir qué uso se da a nuestra información personal?

384 respuestas



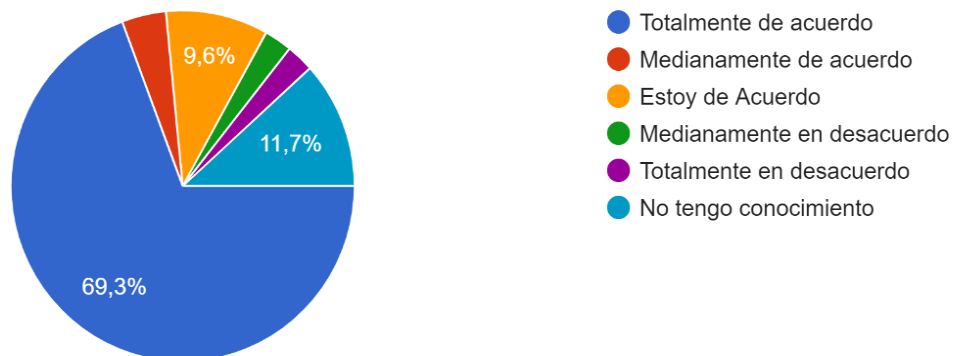
16.- ¿Usted cree que debería de existir un derecho en el que toda la información que usted haya generado o compartido sea eliminada de las bases de datos, tanto privadas como gubernamentales?

384 respuestas



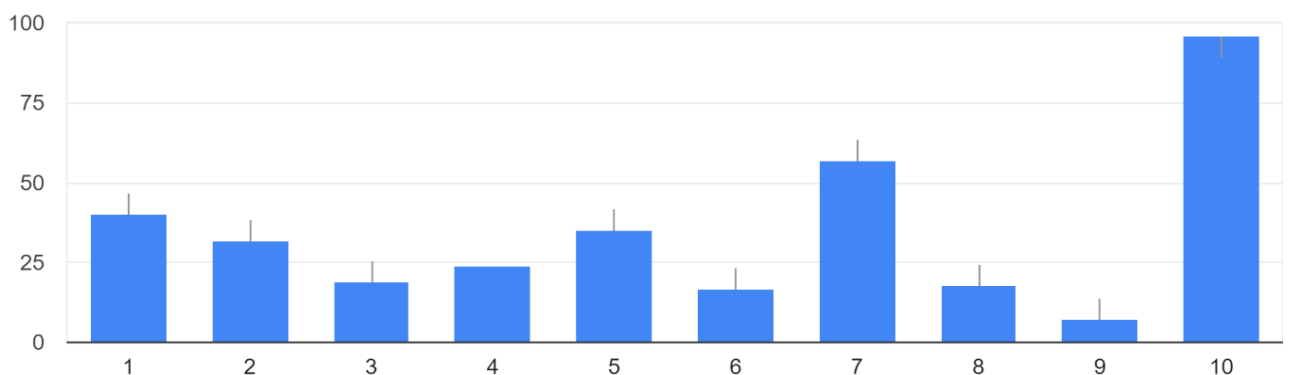
17.- ¿Usted considera que, con el avance de la tecnología, deberíamos tener derecho a decidir qué uso se da a nuestros datos o información personal?

384 respuestas



18.- En una escala del 1 al 10 siendo el 1 lo más bajo y 10 lo más alto, que tan capacitadas cree que se encuentran las instituciones públicas del Ecu...lema y proteger la información de sus ciudadanos?

345 respuestas

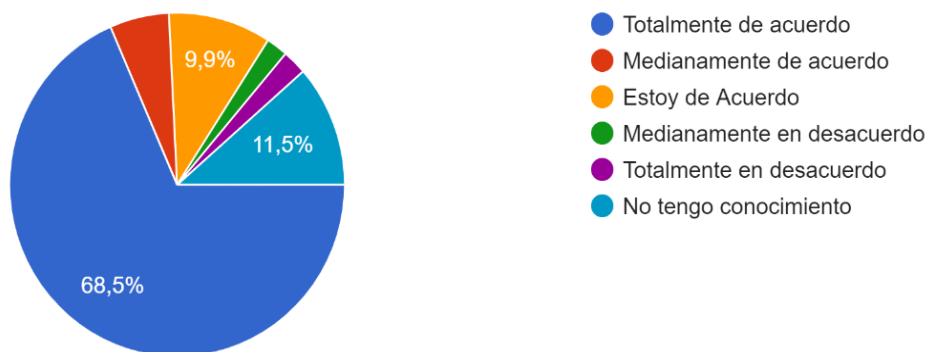


41 respuestas



19.- ¿Cree usted que la Asamblea Nacional del Ecuador debe de preocuparse por legislar en el área tecnológica que involucre al ser humano, entre ell...s personales y seguridad de información personal?

384 respuestas



Anexo 3. Entrevista a expertos sectoriales.

ENTREVISTA PARA DETERMINAR SI EL ACCESO A LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TICS) COMO DERECHO ESTABLECIDO EN LA CONSTITUCIÓN DEL ECUADOR DE 2008 Y SU EFECTO SISTEMÁTICO DE VULNERACIÓN DE DERECHOS DE LOS CIUDADANOS.

Agradecemos su participación en esta encuesta que tiene la finalidad de conocer la opinión de la ciudadanía ecuatoriana en lo que respecta a la conciencia que tiene sobre la protección de sus datos, así como sus derechos, al momento de utilizar las TICs y Redes Sociales. Los datos serán utilizados con fines académicos para la investigación que se titula: "El acceso a las tecnologías de la información y comunicación (TICs) como derecho establecido en la constitución del Ecuador de 2008 y su efecto sistemático de vulneración de derechos de los ciudadanos.

Toda la información que usted nos facilite permanecerá en total confidencial y anonimato. Por tal motivo y agradeciéndole con su participación y colaboración ponemos a consideración el siguiente cuestionario. Si tiene alguna duda con respecto a las preguntas, por favor solicitar una aclaración de las mismas con el entrevistador

Atte.:

Abg. Omar Altamirano Villena.

MAESTRANTE EN DERECHO CONSTITUCIONAL.

Entrevista elaborada desde julio del 2021.

Nombre y Apellidos del entrevistado:

Título Universitario

Abogado

Ingeniero en Sistemas, TIC o afines

Actividad de su profesión:

1. En base al derecho contemplado en el numeral 2 del Art. 16 de la Constitución del Ecuador que determina: "Todas las personas, en forma individual o colectiva, tienen derecho a: El acceso universal a las tecnologías de información y comunicación". ¿Cree usted que su ejercicio tendría como efecto la vulneración de otros derechos de los

ciudadanos, contemplados en la Constitución y Tratados Internacionales de Derechos Humanos? ¿Cuáles? y ¿Por qué? (Desarrolle su respuesta)

2. ¿Cómo cree usted que las Tecnologías de la Información y Comunicación (TICs), Redes Sociales y aplicaciones tecnológicas, ¿causan o causarían violación de derechos a los usuarios? ¿Cuál sería el proceso para esto? (Desarrolle su respuesta)

3. ¿Qué opinión le merece, el uso que las empresas desarrolladoras de tecnología y el Estado dan a los datos o información obtenida de los usuarios, mediante cualquier plataforma tecnológica? (Desarrolle su respuesta)

4. Como experto, que situaciones pueden realizarse con la información o datos recopilados por el sistema de cámaras de seguridad instalada en áreas públicas por el Estado? ¿Esto, podría afectar de alguna manera a los derechos de los ciudadanos? (Desarrolle su respuesta)

5. ¿Cuál es su opinión sobre el uso que se podría dar a los datos que recolectan las Empresas y el Estado. ¿Tiene alguna consecuencia negativa en relación a los derechos de los ciudadanos? (Desarrolle su respuesta)

6. ¿Cómo usuario de internet y redes sociales, cree que la información o datos personales proporcionada por usted, ¿serviría para se configure la violación de sus derechos? ¿Cuáles derechos sería y por qué? (Desarrolle su respuesta)

7. ¿Cree que la práctica de recolección de datos mediante cookies o métodos de captación de información adicional es indiscriminada, al recopilar datos sin conocimiento ni consentimiento del usuario? ¿Qué puede provocar? (Desarrolle su respuesta)

8. Para el usuario, ¿Qué consecuencias traería la recolección de sus datos por parte de empresas y entidades gubernamentales? ¿Conoce el proceso? (Desarrolle su respuesta)

9. ¿Tiene conocimiento si la recolección de información de datos digitales está normada legalmente por el Estado Ecuatoriano? (Desarrolle su respuesta)

10. ¿Cree usted que el Estado Ecuatoriano debería de normar el uso, captación y venta de datos de usuarios por parte de la Empresas desarrolladoras tecnológicas y de las entidades gubernamentales? (Desarrolle su respuesta)

11. ¿Considera que el desarrollo de las TICs, software y programas como la inteligencia artificial podrían vulnerar derechos? ¿Cuáles y por qué? (Desarrolle su respuesta)

12. En su opinión, ¿Cuál sería, la forma óptima y segura de utilizar las TIC, Redes Sociales y Aplicaciones tecnológicas? para evitar la captación de nuestra información y no ser víctimas de vulneración de derechos? (Desarrolle su respuesta)


Anexo 4. Resultados individuales de la entrevista desarrollada a expertos sectoriales.

Resultado de la información levantada por el análisis de la investigación cualitativa desarrollada mediante Altas T.I.


Informe creado por Omar Altamirano en 17/8/2021

Informe de códigos

Todos los (20) códigos

 ○ 08/13/2021 15

1 Citas:

 1:17 ¶ 2 – 9 in Case 1

08/13/2021 15:46:39

Nombre y Apellidos del entrevistado

Amado Joselito Romero Galarza

Título Universitario

Abogado

Actividad de su profesión

Juez de la Sala Civil de la Corte Provincial del Guayas

1.

◇ ○ 1. En base al derecho contemplado en el numeral 2 del Art. 16 de la Constitución del Ecuador que determina: "Todas las personas, en forma individual o colectiva, tienen derecho a: El acceso universal a las tecnologías de información y comunicación". Cree usted que su ejercicio tendría como efecto la vulneración de otros derechos de los ciudadanos, contemplados en la Constitución y Tratados Internacionales de Derechos Humanos? ¿Cuáles? y ¿Por qué? (Desarrolle su respuesta)

20 Citas:

☰ 1:5 ¶ 10 in Case 1

No, por qué no se visualiza la violación de derechos con el acceso a las TIC, más ayuda a desarrollar tareas en el ámbito educativo y laboral

☰ 2:5 ¶ 10 in Case 2

No se considera que vulneraría derechos porque es una declaración de carácter general que más bien facilita el desarrollo y ejercicio de otros derechos constitucionales

☰ 3:5 ¶ 10 in Case 3

Depende del alcance y si existe a la violación a la intimidad, sino existe, no hay violación de derechos


☰ 4:5 ¶ 10 in Case 4

No, porque el acceso a tales tecnologías implica el uso de esas plataformas digitales y sus utilidades o beneficios. No se vulneraría ningún derecho de otra persona, esto en virtud que la información personal que decide la persona alimentarla al sistema o plataforma es por cuenta propia.


☰ 5:5 ¶ 10 in Case 5

Considero que todo derecho, no llega hacer absoluto puesto que el propio alcance de la norma jurídica es otorgar la facultad de goce al sujeto del derecho pero al mismo

tiempo va inmerso el deber jurídico por cuyo motivo si se usa en forma indiscriminada el derecho al uso a las TICs podría violentarse derechos de otros ciudadanos.

 **6:5 ¶ 10 in Case 6**


No, porque es el acceso a las tecnologías, más no a datos privados de otras personas

 **7:5 ¶ 10 in Case 7**


Sí. Uno de los derechos en mayor riesgo es a la intimidad, otro es al buen nombre, otro es a la inviolabilidad de correspondencia. La masificación de la gratuidad sin restricciones genera la filtración de información que, por su naturaleza, es sensible con relación a la condición de "persona", de allí que la ausencia de filtros o cláusulas de permisibilidad de uso (que no formen parte de contratos de adhesión), son puertas abiertas (o ventanas al menos) para que terceros potencialmente accedan, usen y exploten dicha información en perjuicio de su titular.

 **8:5 ¶ 10 in Case 8**


No, si se maneja de manera responsable dicho acceso

 **9:5 ¶ 10 in Case 9**


Sí. Porque la rapidez que caracterizan estas comunicaciones tecnológicas hace que la información se distorsione y pueden afectar el honor de las. Personas, su privacidad

 **10:5 ¶ 10 in Case 10**


no, el derecho al acceso a las tecnologías de información no vulnera otros derechos, porque el acceso nos permite tener mejores y más conocimientos en el área que se necesite y esa información lo puede convertir una persona más productiva generador de ingresos y por lo tanto ayuda a la economía de un país.

 **11:5 ¶ 10 in Case 11**


No, la información es pública, pero hay grupos de personas que la usan para hacer daño

 **12:5 ¶ 10 in Case 12**


Por una parte nosotros como usuarios de Internet y redes sociales damos con mucha facilidad nuestra información personal, y por otra parte los. Dueños de las redes sociales y el Internet se aprovechan de esto y prácticamente están violentando nuestra privacidad

 **13:5 ¶ 10 in Case 13**


Todos debemos tener acceso a las canales de tecnología, los datos no deben ser vulnerables y guardar el sigilo confidencial.

 **14:5 ¶ 10 in Case 14**


No sé considera en si, una vulneración de derechos por que no es una declaración de derecho general, por tanto no considero que vulnere los derechos como tal.

 **15:5 ¶ 10 in Case 15**


No tendría ninguna vulnerabilidad siempre y cuando no se viole la privacidad de la información

 **16:5 ¶ 10 in Case 16**


Si, el derecho a la privacidad. Siempre y cuando, los acuerdo que se acepten, al estar en las RRSS, estén bien claros y sean de conocimiento pleno de quienes ingresan a estos servicios.

 **17:5 ¶ 10 in Case 17**


Derecho a Vivir: Vida en Armonía, Paz con uno mismo y con los demás.
Derecho a la intimidad: Vida sin control en redes sociales donde se distorsiona los valores.
Derecho a no tener conocimientos de valores morales: Sabemos que la tecnología tiene la oportunidad de llenar los vacíos inmorales y no se da buena moral.

 **18:5 ¶ 10 in Case 18**


Si, a la seguridad y privacidad de la información. Hoy en día las Tics están inmersas tanto en el ámbito laboral cómo estudiantil de las personas, más aún en la actualidad a raíz del covid 19 el estado debe de garantizar el acceso universal y privacidad a las tecnologías de información y comunicación para poder desarrollar las actividades de los ciudadanos.

 **19:5 ¶ 10 in Case 19**

No creo porque más bien con el acceso universal se está disminuyendo la brecha digital

 **20:5 ¶ 10 in Case 20**

Se debe restringir los accesos a la creación de las cuentas en Redes Sociales porque hay muchos perfiles falsos y son utilizados para estafar a personas.

 ○ **10. ¿Cree usted que el Estado Ecuatoriano debería de normar el uso, captación y venta de datos de usuarios por parte de la Empresas desarrolladoras tecnológicas y de las entidades gubernamentales? (Desarrolle su respuesta)**

20 Citas:

 **1:14 ¶ 28 in Case 1**

Si, la información de los ciudadanos no podría estar en manos de personas particulares que hagan uso comercial de las mismas

 **2:14 ¶ 28 in Case 2**

Es urgente estamos expuestos al uso de nuestra información personal

 **3:14 ¶ 28 in Case 3**

Si debe ser normada porque violan su intimidad, llegando hasta desarrollarse el acoso

 **4:14 ¶ 28 in Case 4**

Estoy de acuerdo que se deban normar el uso de captación y venta de datos ya que es indiscriminado.

 **5:14 ¶ 28 in Case 5**

Debería de ser prohibido ya que vulnera la privacidad de información personal

 **6:14 ¶ 28 in Case 6**

Debería de ser más transparente la entrega de éste tipo de datos para poder conocer, quién los entregó y quién los recibió, así mismo debería de existir suficiente información que indique en qué lugar se puede encontrar al que está haciendo uso de la información de manera que pueda responder de ser necesario, a esto debe de agregarse la agilidad en el proceso respectivo de reclamo.

 **7:14 ¶ 28 in Case 7**

Sí. Debe tutelar la opción de negarse a compartir información irrelevante por ejemplo. A saber: si todos mis bienes inmuebles deben ser inscritos en el registro de la propiedad donde se encuentren, la entidad que desea saber información al respecto, debe hacer su gestión investigativa, y no obligarme a darle los detalles como fecha de la escritura, precio, etc. Dicho de otra forma, se debe promover la eficiencia en la interacción entre entidades públicas, v.g. municipios, registradores, entes de control.

 **8:14 ¶ 28 in Case 8**

Creo que debe limitarse el acceso y uso, y por supuesto normar actividad, pero, debe prohibirse la captación y venta de datos de usuarios, eso debe estar restringido a fines legales o salvo la voluntad de cada persona que acepte que su información sea compartida

 **9:14 ¶ 28 in Case 9**

Claro!

 **10:14 ¶ 28 in Case 10**

Claro que si debe normar empezando por la captación de datos y deben estar en continua actualización y mejoras, ya que siempre las empresa buscaran evadir las reglas

 **11:14 ¶ 28 in Case 11**

Así es para que la información sea correcta y protegida

 **12:14 ¶ 28 in Case 12**

Así es, creo que el estado Ecuatoriano debe normar estas situaciones

 **13:14 ¶ 28 in Case 13**

Si debe normal la privacidad de información

 **14:14 ¶ 28 in Case 14**

Si lo considero, para que de esta manera no violen nuestros derechos

 **15:14 ¶ 28 in Case 15**

Si

 **16:14 ¶ 28 in Case 16**

Por supuesto que si.

 **17:14 ¶ 28 in Case 17**

Si deberia de normar el uso, el estado tiene la obligación de controlar todas estas normativas.

 **18:14 ¶ 28 in Case 18**


Si debería normar ya que el estado debe de garantizar la seguridad del ciudadano

 **19:14 ¶ 28 in Case 19**

Totalmente de acuerdo, se debe precautelar la privacidad de datos del usuario

 **20:14 ¶ 28 in Case 20**

El Estado Ecuatoriano a través de leyes debe controlar la captación y venta de datos.

 **11. ¿Considera que el desarrollo de las TICs, software y programas como la inteligencia artificial podrían vulnerar derechos? Cuáles y por qué? (Desarrolle su respuesta)**

20 Citas:

 **1:15 ¶ 30 in Case 1**

Generan vulneración de derechos, como el derecho a la intimidad, honra y buen nombre

 **2:15 ¶ 30 in Case 2**

Si y de hecho ya lo vulnera, pues la ciencia avanza más rápido que la normativa ya que es lento su proceso

 **3:15 ¶ 30 in Case 3**

No ya que depende de uso

 **4:15 ¶ 30 in Case 4**

El desarrollo tecnológico es amplio, abarcando infinidad de ambientes en los que se desarrolla el ser humano, sin duda merece un mayor control a efecto que exista una limitación consentida por el usuario, persona o ciudadano. Los derechos que se podría

afectar son el derecho a la intimidad, el derecho a decidir sobre si, derecho a tomar decisiones libres y responsables sobre la salud, el uso de las infinidades de aplicaciones afecta la salud del ser humano.

 **5:15 ¶ 30 in Case 5**

Los avances tecnológicos por el alcance pueden violentar particularmente el derecho a la privacidad e intimidad

 **6:15 ¶ 30 in Case 6**

Siempre es un riesgo que seguramente van a ocurrir que afectaran al derecho de la privacidad principalmente. Pero debemos de entender -lo que quizás nos cueste bastante lo que todo esto es parte de la evolución de la humanidad. Éste tema habría sido ciencia ficción hace apenas cien años y es muy posible que cien años después todo lo que ahora nos asusta sea considerado tecnología obsoleta.

 **7:15 ¶ 30 in Case 7**

Ver respuesta 1.

 **8:15 ¶ 30 in Case 8**

El uso responsable no, la manipulación de sistemas si, por ello debe estar debidamente establecido en la ley

 **9:15 ¶ 30 in Case 9**

Podría. Siempre puede haber esa posibilidad si no se regulan esos programas

 **10:15 ¶ 30 in Case 10**

no, la ciencia no vulnera derechos, el mal uso que las personas le dan aun producto obtenido por la ciencia es la que podría vulnerar algún derecho, por ejemplo: si se crea un robot que sea facturador-cajero va ayudar a esa empresa, pero si esa empresa despide a sus cajeros sin cumplir con sus derechos o los cambia a otra área, no es un

tema del producir creado es el ser humano que hace con ese producto, por ello todo debe estar normas y con reglas establecidas por el estado

 **11:15 ¶ 30 in Case 11**

No existe vulneración si la información está protegida

 **12:15 ¶ 30 in Case 12**

Si considero q puede violar nuestro derecho a tener nuestra privacidad

 **13:15 ¶ 30 in Case 13**

Hoy en día cada vez estamos viendo que los procesos son automatizados a la inteligencia artificial no considero vulneración si se utiliza las seguridades correctas.

 **14:15 ¶ 30 in Case 14**

El derecho a la honra y al buen nombre, a la libertad

 **15:15 ¶ 30 in Case 15**

Podrían vulnerar derecho siempre y cuando la seguridad de la misma no sea la apropiada

 **16:15 ¶ 30 in Case 16**

Claro que sí. La inteligencia artificial (IA) ha evolucionado demasiado, al punto de que se alimenta con Big Data, que refieren al estudio de comportamiento, como una de tantas opciones de uso. Por ende, las tecnologías simplemente actúan basadas en patrones y, aunque no estoy seguro de que sea un derecho, se violaría el libre albedeío; ya que habrá un determinado momento, en donde algo que siempre realizo, ya no lo pueda hacer y sin embargo, la tecnología lo hizo sin mi conocimiento.

 **17:15 ¶ 30 in Case 17**

Si, podrían vulnerar y porque se sabría todo acerca de las personas. Lo que se debería ver es limitaciones.

 **18:15 ¶ 30 in Case 18**


Toda herramienta tecnológica en donde se suministran y almacenan datos e información de usuario puede ser causa de alguna u otra manera de vulnerabilidad de privacidad de usuario

 **19:15 ¶ 30 in Case 19**


Si, si cae en manos de grupos inescrupulosos; pero bien intencionados permite explorar nuevos conocimientos al hombre

 **20:15 ¶ 30 in Case 20**


Las Aplicaciones son buenas si se emplean de buena manera y no se vulneraría derechos.

 **○ 12. En su opinión, ¿Cuál sería, la forma óptima y segura de utilizar las TIC, Redes Sociales y Aplicaciones tecnológicas? para evitar la captación de nuestra información y no ser víctimas de vulneración de derechos? (Desarrolle su respuesta)**


20 Citas:

 **1:16 ¶ 32 in Case 1**

Es necesario eliminar mecanismos que no permitan rastrear al ciudadanos

 **2:16 ¶ 32 in Case 2**

Que la adquisición y uso de las plataformas deba ser autorizado de forma expresa, conociendo en todos los detalles de la información que va hacer usado por las empresas y estado.

 **3:16 ¶ 32 in Case 3**


No existe una forma segura de utilizar ya que el problema no es elevar información, sino que existe personas, ya sean los que trabajan en las empresas tecnológicas o hackers que hacen mal uso de los datos personales.

 **4:16 ¶ 32 in Case 4**


Ser consciente de la información que publiquemos. Ser responsable de las claves de acceso a los aplicativos que dispongo o uso. Conservar respaldos de los formularios y de las cookies que he autorizado a efecto de conocer a ciencia cierta llegado el momento apropiado que es lo que he autorizado y de qué forma.

 **5:16 ¶ 32 in Case 5**


Mantener una regulación y que los organismos del estado encargado de su manejo puedan contar con fórmulas de control y protección.

 **6:16 ¶ 32 in Case 6**

No creo que haya manera de hacerlo, el humano es un ser sumamente inteligente y siempre va a encontrar la manera de ir más allá de lo que permiten las regulaciones. Por otro lado la imposición de normativas siempre es lenta, debido a la cantidad de procesos que tienen que pasarse antes de ser aprobadas. Los hechos siempre llegan antes que el derecho.

 **7:16 ¶ 32 in Case 7**

Ver respuesta 10.

 **8:16 ¶ 32 in Case 8**

Bajo la legislación amplia y clara sobre su uso, y bajo la autorización de cada individuo, para fines estatales y legales, limitando su uso y supervisando la información que contenga, sería la manera más óptima de utilizar las TIC. El internet y las redes sociales son un gran poder, puede ser muy beneficioso es verdad, nos permite estar actualizados y tener noticias en segundo la, pero en manos equivocados puede generar incertidumbre y gran daño social.

 **9:16 ¶ 32 in Case 9**

Ser prudentes. No autorizar la captación

 **10:16 ¶ 32 in Case 10**

Cada plataforma tiene opciones de configuración de seguridad privacidad y debemos aprender a utilizarlas y no publicar datos personales que no tienen por qué conocerlos todo el mundo

 **11:16 ¶ 32 in Case 11**

Conocer la plataforma antes de ingresar datos personales

 **12:16 ¶ 32 in Case 12**

Considero que eso debe hacerlo el estado con ayuda de expertos en tecnología y personal ético de marketing

 **13:16 ¶ 32 in Case 13**

Un buen ruteo y montaje de firewall para evitar captación de datos.

 **14:16 ¶ 32 in Case 14**


Deberían de buscar o emplear algún método para que de esta manera no vulneren nuestras vidas, intimidad y nuestra privacidad

 **15:16 ¶ 32 in Case 15**

Utilizar los recursos de hardware y software adecuadamente

 **16:16 ¶ 32 in Case 16**


Estar completamente seguros de los acuerdos que aceptamos al utilizarlas y tener plena consciencia de lo que publico, valorando riesgo/beneficio.

 **17:16 ¶ 32 in Case 17**


Ponerle límites a cada aspecto que se vaya a requerir los datos, ejemplo: al momento de la compra en un establecimiento, datos a facturar.

 **18:16 ¶ 32 in Case 18**


Tratar por parte de los usuario no suministrar datos e información sensible que pueda causar conflictos de privacidad y el estado debe de normar esto para que en caso de vulnerabilidad de información se pueda dar opción al ciudadano de hacer su reclamo

 **19:16 ¶ 32 in Case 19**


Qu exista una huella ética en cada individuo a través de la capacitación y consecución consciente de los puntos vitales buenos y malos del uso de este derecho

 **20:16 ¶ 32 in Case 20**


Las cuentas de las redes sociales deben ser autorizadas por parte del Registro Civil para que no haya perfiles falsos.

 ○ **2. ¿Cómo cree usted que las Tecnologías de la Información y Comunicación (TICs), Redes Sociales y aplicaciones tecnológicas, causan o causarían violación de derechos a los usuarios?Cuál sería el proceso para esto? (Desarrolle su respuesta)**

20 Citas:


 **1:6 ¶ 12 in Case 1**

Para acceder a un programa solicitan una autorización y por lo tanto se debe sujetarse a un contrato de adhesión para su utilización, por lo que está en el usuario el derecho de acceder o no a las mismas


 **2:6 ¶ 12 in Case 2**

La violación se produciría o se produce por la falta de regulación y control (obviamente enmarcado en la constitución) por lo que estos derechos deben ser


armonizados con otros derechos para no afectarlos por ejemplo a algunos detallados en el Art. 66 de la Constitución del Ecuador.

 **3:6 ¶ 12 in Case 3**


No creo que causen violación a ningún tipo de derecho, ya que todos tienen derecho a publicar la información que considere, la vulneración de derechos desarrollaría al exponer información de una tercera persona

 **4:6 ¶ 12 in Case 4**


Cuando el administrador de tales aplicativos sin consentimiento venda mi información personal o a través de datos. Cuando otras personas o usuarios difunden información que atenta contra la dignidad y la honra de la persona afectada. Cuando por tales aplicativos se proceda a la localización o ubicación de la persona.

 **5:6 ¶ 12 in Case 5**


Particularmente porque permiten acceder a las mismas, en algunos casos refugiándose en identidades falsas y que en muchos de los casos resulta difícil o imposible identificar.

 **6:6 ¶ 12 in Case 6**


Es posible que esto ocurra por los llamados hackers, con lo que obviamente debe ser controlado por gente especializada. Sin embargo, si bien creo que debe existir un control, no debería haber una alarma exagerada, porque al fin y al cabo es un delito. Al igual que asaltar a una persona en la calle y robar sus pertenencias, quien hakea invade la privacidad de otra persona. Ambos son actos ilícitos.

 **7:6 ¶ 12 in Case 7**


Al momento que se permite el uso ilimitado, sin rastro de responsabilidad o identificación fidedigna del consumidor que accede a determinada información a través de las TiCS, se crean espacios para que tales sean utilizadas libremente.

 **8:6 ¶ 12 in Case 8**


Cuando se usa para victimizar en circunstancias aún no sentenciadas, el uso mediático de las redes y la información puede ser el más grande problema

 **9:6 ¶ 12 in Case 9**


Por la Rapidez y porque hay personas que no reparan en que desconocen algún tema e igual emiten criterios equivocados

 **10:6 ¶ 12 in Case 10**


Cuando públicas o tergiversar información que no te pertenece, y para eso existen leyes que lo regulan, lo que se debería hacer es aplicar bien las leyes cuando correspondan, y no por el llamado derecho a la expresión hagan lo que quieran, el problema no es el acceso a la tecnología el tema es lo que haces con ellas, si respetas las leyes y las reglas que existe, no vulnerarias derechos

 **11:6 ¶ 12 in Case 11**


Cuando se filtra información que no debe ser pública

 **12:6 ¶ 12 in Case 12**


Ellos con la información personal obtenida se benefician económicamente, además pueden manipular y persuadir a las personas y así obtiene beneficios económicos

 **13:6 ¶ 12 in Case 13**


Cada persona es repónganles de la información dada en sus redes sociales o ingreso de datos a aplicaciones no es una violación si tienes un perfil público y lo compartes, la app tienen niveles de seguridad para tu como usuario te protejas.

 **14:6 ¶ 12 in Case 14**


No considero que violen tus derechos como tal

 **15:6 ¶ 12 in Case 15**


La filtración de información está sujeta a la seguridad que brindan las empresas encargadas de tener a cargo la administración de la seguridad de la información

 **16:6 ¶ 12 in Case 16**


Desde el punto de vista cuentas personales: Todas las aplicaciones tienen restricciones y seguridades, las que el propietario debe ser conocedor. Esto restringe el acceso a q otros usuarios "ataquen" al propietario de la cuenta. Se debe capacitar para crear una cuenta en cualquier red social. Desde el punto de vista de que si alguien fue grabado o usado su imagen para causar daño a la integridad, esto debe ser penalizado y aunque en la ley lo define, las personas que difunden esto no tienen conocimiento de la causa. Se debe hacer campañas de concientización y explicar que pasa en el caso de que alguien virilice algo para hacer un daño a determinada entidad o persona.

 **17:6 ¶ 12 in Case 17**


Invadiendo la privacidad por medio de una compañía de telecomunicaciones en llamadas, mensajes. Y además con inteligencia artificial se sabría todo en detalle. Afectando la parte emocional y económica de las personas. Uno de los procesos a realizar podría ser en la cédula de identidad con actualizaciones en base a 7 puntos personales. (Únicamente por el usuario)

 **18:6 ¶ 12 in Case 18**

Tal vez por la privacidad de la información suministrada en redes sociales y aplicaciones tecnológicas, puesto que empresas grandes como FaceBook se ha evidenciado que venden bases de datos de usuarios a terceros para lucrarse de ello

 **19:6 ¶ 12 in Case 19**

Si causarían si no se ponen reglas claras que eviten el abuso de su uso de parte de ciertos usuarios o grupos de usuarios

 **20:6 ¶ 12 in Case 20**

Los perfiles falsos son empleados para acceder a información privada.

◇ ○ 3. ¿Qué opinión le merece, el uso que las empresas desarrolladoras de tecnología y el Estado dan a los datos o información obtenida de los usuarios, mediante cualquier plataforma tecnológica? (Desarrolle su respuesta)

20 Citas:

☰ 1:7 ¶ 14 in Case 1

La captación de información de los usuarios expone al ciudadano a que sus datos puedan ser utilizados por corporaciones o estados para un control social o venta de información respecto de los gustos de los clientes o usuarios.

☰ 2:7 ¶ 14 in Case 2

Es un abuso el que realizan, deben ser normados y regulados

☰ 3:7 ¶ 14 in Case 3

No afecta ningún ni vulneran ningún tipo de derecho, ya que sea compañías de seguridad y comunicación legal mente constituida

☰ 4:7 ¶ 14 in Case 4


Abusiva esto por cuanto el consumidor de tales preformas tiene la única oportunidad de aceptar las condiciones que llevan implícitas, que si no aceptan las mismas, simplemente no puede usar el servicio. Impidiendo al actuario que pueda sobre ciertas cuestiones inherentes a la persona, esta pueda decidir si la acepta o no.

☰ 5:7 ¶ 14 in Case 5


Es también un abuso de la información pues el usuario si bien es cierto se somete a contrato de adhesión al aceptar as condiciones sin embargo se violenta un derecho al otorgar la información a terceros

☰ 6:7 ¶ 14 in Case 6


Pienso que en muchas ocasiones resulta hasta corrupto. Ocurre consuetudinariamente que recibo llamadas a mi línea celular, ofreciéndome cambiar de operador, quién les dio mi número de teléfono y quien le dio derecho a llamar. Eso obviamente invasión al derecho a la privacidad, cómo dije debe de ser controlada.

 **7:7 ¶ 14 in Case 7**


Mediocre pues no hay seguridad acerca de la confidencialidad debida. Y aunque tecnológicamente exista dicha seguridad, debido a las cláusulas de adhesión de ciertas empresas privadas, se reservan el derecho de transmitir la información de sus usuarios a las demás empresas que forman parte de sus grupos económicos, de manera que el proveedor de telefonía celular que también vende electrodomésticos, y también televisión por cable, internet, etc, les da a todos sus gerentes las facilidades para contactarnos durante sus campañas promotoras de tales bienes o servicios adicionales. Simplemente es invasivo.

 **8:7 ¶ 14 in Case 8**


Al ser Casi ilimitadas, deben tener parámetros de uso que no interfiera en los derechos de los usuarios sin su consentimiento

 **9:7 ¶ 14 in Case 9**


Es un uso muy amplio, que afecta la privacidad

 **10:7 ¶ 14 in Case 10**


el estado y la empresa privada, debe garantizar que la información de los ciudadanos que no es pública este segura, pero resulta que la información de teléfonos, correos que das para una factura por ejemplo ya la tienen para toda campaña de marketin, ventas etcétera tu información se divulga sin ninguna responsabilidad eso no es correcto.

 **11:7 ¶ 14 in Case 11**


Mientras la información se encuentre protegida estaría bien

 **12:7 ¶ 14 in Case 12**


Creo q esa información debería ser manejada de manera diferente por parte de las mencionadas empresas, debe haber un poco más de restricción por parte de los gobernantes de cada país

 **13:7 ¶ 14 in Case 13**


Existen contratos de confidencialidad cuando se esta desarrollando y debe ser estipulada correctamente y evitar a futuro que las BD sean ofertadas para fines de marketing

 **14:7 ¶ 14 in Case 14**


Que todas las empresas hagan y capten todos tus datos eso si es una violación a tu privacidad

 **15:7 ¶ 14 in Case 15**


La seguridad es deficiente, presenta falencias especialmente en el sector público

 **16:7 ¶ 14 in Case 16**


Depende lo que estipule el acuerdo que la plataforma desarrolladora pone previo a la aceptación del servicio. Generalmente no lo leen. Es un gran problema eso. Las empresas que desarrollan esto no deben dar la data a nadie mi opinión personal.

 **17:7 ¶ 14 in Case 17**


La tecnología puede tener su avance pero el Estado no está preparado debido a la corrupción que se ha visto.

 **18:7 ¶ 14 in Case 18**


La privacidad e integridad de los datos es parte fundamental de cada usuario que da uso de herramientas tecnológicas como aplicaciones, redes sociales, etc

 **19:7 ¶ 14 in Case 19**


Está bien siempre y cuando no lesione al individuo, y que sea con conocimiento consciente del usuario

 **20:7 ¶ 14 in Case 20**


La información debe ser privada y se debería regular para que las empresas vendan la información.

 ○ **4. Cómo experto, que situaciones pueden realizarse con la información o datos recopilados por el sistema de cámaras de seguridad instalada en áreas públicas por el Estado? Esto, podría afectar de alguna manera a los derechos de los ciudadanos? (Desarrolle su respuesta)**


20 Citas:

 **1:8 ¶ 16 in Case 1**


El desarrollo tecnológico a llevado a que la humanidad tenga que pagar un precio por el mismo lo que conlleva a que los ciudadanos pierdan parte de su privacidad a través de la recuperación de información

 **2:8 ¶ 16 in Case 2**

Si, afecta el derecho a la libertad, intimidad, libre circulación y de tránsito

 **3:8 ¶ 16 in Case 3**

No, todo lo contrario me parece que Sería bastante bueno ya que se controla a la delincuencia

 **4:8 ¶ 16 in Case 4**

Pensando en que el Estado es responsable de la seguridad interna y externa y que dado el actual estado de desarrollo tecnológico exige mayores condicionantes que permitan identificar personas para su identificación, localización y ubicación, el estado

estaría fijando parámetros mayores de seguridad. Pero éstos si se encontrarían limitados por un principio de confidencial al uso exclusivo de un gobierno, en dónde no debería difundir abiertamente tales señales o recepción de señales, imágenes, audio voz inherente a la persona en particular, salvo que existiera orden expresa de autoridad pública para que se use tal información, por ejemplo cuando se dan las suertes en la penitenciaria y la forma de sus actos delincuenciales son difundidas a la ciudadanía, no debería de difundirse, sino almacenarse y otorgar a la fiscalía, para uso de particulares fines.

5:8 ¶ 16 in Case 5


Siendo la persona un sujeto del derecho y de deber jurídico al mismo tiempo su accionar público debe estar dentro de las normas jurídicas a la moral y las buenas costumbres de allí que existiendo la necesidad de brindar protección al ciudadano, se pueda establecer mecanismos de control y en la era actual hacer uso de la tecnología lo que estando consiente el ciudadano de ese particular si la información es utilizada solo con esos fines y no distorsionado su uso no afectaría a derecho alguno. Tanto más que para fines de investigación se debe de realizar con las partes procesales.

6:8 ¶ 16 in Case 6


No creo que se vulneran derechos por ello, las cámaras de seguridad están ubicadas en lugares públicos y todo ciudadano sabe muy bien, estando en un lugar público, sus actos están a la vista de todos. Para ponerlo de otra manera, si un ciudadano comete un ilícito que es captado por las cámaras de seguridad no podría alegar violación al derecho a su privacidad, porque lo mismo podría alegar si fuese un testigo, con el absurdo argumentó que el testigo no debería de ver su vida privada.

7:8 ¶ 16 in Case 7


Las áreas públicas están expuestas al control. De manera que todo lo relacionado o derivado de dicho control, siempre que esté asociado a la protección del bien jurídico seguridad, orden y paz, es adecuado.

 **8:8 ¶ 16 in Case 8**


Es posible que surja alguna afectación, pero ese dependería de cada caso en particular, ya que también contribuye al control de seguridad ciudadana

 **9:8 ¶ 16 in Case 9**


Pueden dar lugar a delitos como extorsión, robo, difamación

 **10:8 ¶ 16 in Case 10**


no afecta en el sentido de seguridad, ayuda a identificar cualquier acto anómalo que pudiera existir y en muchos casos sirve de descargo hasta para el mismo ciudadano, en caso si le robaron dentro de las instalaciones, o lo agredieron, o donde estuvo en un día específico, aunque la información de cámaras de vigilancia siempre tienen un tiempo determinado, el mal uso que se dé a esta información ya depende del estado.

 **11:8 ¶ 16 in Case 11**


No, porque las cámaras públicas ayudan a controlar los sucesos que causan daño a la sociedad

 **12:8 ¶ 16 in Case 12**


Considero que las cámaras de seguridad por parte del estado si ayudan y mucho para el beneficio de los ciudadanos ya que de esta manera quedará registrado cualquier acto de violencia o ataque o accidente de tránsito etc y esto es de mucho beneficio

 **13:8 ¶ 16 in Case 13**


Más que afectación son soportes válidos para causas procesales positivas o negativas.

 **14:8 ¶ 16 in Case 14**


Si, a tu privacidad como ciudadano

 **15:8 ¶ 16 in Case 15**


De ninguna manera siempre y cuando se lo instale en esos lugares estratégicos destinados a brindar seguridad

 **16:8 ¶ 16 in Case 16**


Si se expone por supuesto que si. Solo debería darse en el caso de uso para determinada acción legal o algo que realmente lo amerite.. y con las debidas firmas de compromiso a que la data no sea virilizada.

 **17:8 ¶ 16 in Case 17**


En cuanto a situaciones, podría alterarse la verdad de los hechos. El control es importante, por seguridad y respaldo. No afectaría. al contrario, creería que los ciudadanos deben ser accesibles a este tipo de seguridad debido a cualquier seguimiento.

 **18:8 ¶ 16 in Case 18**


En este aspecto considero que se puede usar de manera positiva la información recopilada por los sistemas de cámaras, para evidenciar algún accidente, robo, asesinato, secuestro que sirva como material de prueba para identificar la situación

 **19:8 ¶ 16 in Case 19**

Pueden servir para alertar activamente o pasivamente actos que vayan en contra de la ley y el orden

 **20:8 ¶ 16 in Case 20**

La información de las cámaras en lugares públicos debe ser de libre acceso para un mejor control de la seguridad.

 1:17 ¶ 2 – 9 in Case 1

08/13/2021 15:46:39

Nombre y Apellidos del entrevistado

Amado Joselito Romero Galarza


Título Universitario

Abogado


Actividad de su profesión

Juez de la Sala Civil de la Corte Provincial del Guayas

1.

 ○ 5. **Cuál es su opinión sobre el uso que se podría dar a los datos que recolectan las Empresas y el Estado. Tiene alguna consecuencia negativa en relación a los derechos de los ciudadanos? (Desarrolle su respuesta)**


20 Citas:

 1:9 ¶ 18 in Case 1


Repercute directamente en el derecho a la intimidad y a una posible utilización de dicha información para fines que atenten contra la dignidad de las personas o su integridad física inclusive la vida

 2:9 ¶ 18 in Case 2


No existe transparencia en el uso de la información, hasta que los ciudadanos activan el aparato judicial por verse afectados

 3:9 ¶ 18 in Case 3


No creo que se vulneren derechos

 **4:9 ¶ 18 in Case 4**


No afectaría a la persona ni a la identidad de ésta, la información nace de la persona y el estado es responsable de conservar y guardar la información proporcionada.

 **5:9 ¶ 18 in Case 5**


Es el uso exclusivamente relacionado a la actividad o servicio que prestan, cumpliéndose con la obligación de mantener la reserva de la obligación

 **6:9 ¶ 18 in Case 6**


El uso es el que lo quieran dar

 **7:9 ¶ 18 in Case 7**


Ver respuesta 3. Además, no porque sean entidades públicas están exentas de ataques piratas como alguna vez lo fue el SRI, ahora CNT.

 **8:9 ¶ 18 in Case 8**


Cuando su uso es ilimitado sin fines establecidos previamente, pueden afectar negativamente, sin embargo, existe información que corresponde a la transparencia que deben aplicar las empedas d instituciones estatales. Se debe identificar la información, el sujeto y el uso

 **9:9 ¶ 18 in Case 9**


Deben usarse los datos de manera prudente

 **10:9 ¶ 18 in Case 10**


el mal uso que se pueda dar es infinito, una vez que tus datos son público le sirve a la gente q se dedica a extorsionar, bandas delictivas, te dejan expuesto a diversidad de eventos, las consecuencias son graves no tienes tranquilidad y vives desconfiando de todo.

 **11:9 ¶ 18 in Case 11**


Que esta bien

 **12:9 ¶ 18 in Case 12**


El estado debería manejar de mejor manera los datos de todos los ciudadanos sin invadir su privacidad

 **13:9 ¶ 18 in Case 13**


Lo negativo es que exista una fuga de datos, pero para esto en los contratos labores se deben incluir de forma clara y detallada que aspectos deben guardarse y no compartirse.

 **14:9 ¶ 18 in Case 14**


Esto repercute de cierta manera a tu intimidad y vida privada

 **15:9 ¶ 18 in Case 15**

Si uso debe confidencial y especialmente destinado al análisis de información más no a la divulgación de la información

 **16:9 ¶ 18 in Case 16**


Pienso que no, debido a que, en términos tecnológicos a esto se lo conoce como Big Data y la misma ya se está aplicando en todas las grandes plataformas que hay. La Big Data nos permite hacer el estudio del comportamiento de las personas. Si hubiese la certeza, lo cual es muy difícil que se dé, y se utiliza esta información para cuestiones como: salud, turismo, consumidor y afines; entonces valdría la pena. Pero imaginemos que la Big Data la usen para malas acciones, entonces sería catastrófico.

 **17:9 ¶ 18 in Case 17**


La vulnerabilidad de los datos.

 **18:9 ¶ 18 in Case 18**


Si, toda información de terceros que sea difundida sin autorización es una violación a la seguridad y privacidad de cada usuario

 **19:9 ¶ 18 in Case 19**

Esta data debería ser bien resguardada para que no caiga en manos de delincuentes; y tampoco debe ser usada para fines políticos

 **20:9 ¶ 18 in Case 20**


Las bases de datos de las personas deben servir para implementar programas de capacitación

 ○ **6. ¿Cómo un usuario de internet y redes sociales, cree que la información o datos personales proporcionada por usted, serviría para se configure la violación de sus derechos? ¿Cuáles derechos sería y por qué? (Desarrolle su respuesta)**

20 Citas:

 **1:10 ¶ 20 in Case 1**

Si, porque a través de estos algoritmos que manejan estas súper computadoras permiten establecer patrones de conducta, frecuencias en cuanto a gusto de las personas

 **2:10 ¶ 20 in Case 2**

Si, por no haber transparencia ni información de mis datos personales

 **3:10 ¶ 20 in Case 3**

No porque en todo caso si yo publico una información es porque quiero hacerla pública y si es publica ano veo que se menoscabe ningún tipo de derecho

 **4:10 ¶ 20 in Case 4**

No, ningún derecho se violaría por cuanto esta información que he entregado o proporcionado obedece a un acto propio de la persona

 **5:10 ¶ 20 in Case 5**

Si, puesto que se violenta particularmente el derecho a la privacidad a no interrumpir su horario de descanso y tranquilidad.

 **6:10 ¶ 20 in Case 6**

Es posible que ocurra. Aún en el caso, de que la empresa que recolecta mis datos no tenga intención alguna de violar mi derecho de privacidad y de compartirlo con otras personas, siempre existe la posibilidad de que alguna persona proceda de modo inadecuado. Éste es un punto muy delicado sobre en quien recae la responsabilidad, cuando ocurre una violación a la privacidad ocasionada con un tercero, ya que es difícil determinar si hay culpabilidad por no cuidar bien de la información o si la habilidad del tercero excede cualquier medida razonablemente aceptable.

 **7:10 ¶ 20 in Case 7**

Ver respuesta 1.

 **8:10 ¶ 20 in Case 8**

Podría ser violatorio cuando se use sin consentimiento y para fines legalmente no establecidos. El derecho a la propiedad, a la seguridad, el buen vivir, entre otros derivados de ellos, por ejemplo cuando se proporciona información del Domicilio y puede ser publicada poniendo en riesgo la seguridad y el acceso a la delincuencia, , partiendo de aquello, varios delitos que pueden ser perpetrados con Información que se filtra para usos indebidos.

 **9:10 ¶ 20 in Case 9**

Podría darse, pero para mí las redes son solo espacios sociales que uso son. Prudencia por mi actividad laboral.

 **10:10 ¶ 20 in Case 10**


las redes sociales la gente la usa como un medio de comunicación pero todo lo que está en la web es utilizada para diferentes temas como campañas de marketing que de acuerdo a tus like en publicaciones ya te envía sugerencia de amistades, cuentas a seguir, paginas a visitar, ya que las multinacionales trabajan con los datos de la red, compran data par su marketing, pero también hay gente que utiliza estos datos que las mismas personas publican par chantajes o para estafas, ya depende de cada persona cuidar q publica así evitarían en algo las vulneración de sus derechos

 **11:10 ¶ 20 in Case 11**

No, porque la información debe ser almacenada bajo las normas de seguridad correspondientes

 **12:10 ¶ 20 in Case 12**

Si considero que las empresas que obtienen nuestros datos si invaden nuestra privacidad y además ellos se benefician económicamente o de cualquier manera q ellos consideren oportuno,

 **13:10 ¶ 20 in Case 13**

Manejando los protocolos de seguridad no hay violación alguna.

 **14:10 ¶ 20 in Case 14**

Si , por que tendrían acceso a toda mi información violando mi privacidad

 **15:10 ¶ 20 in Case 15**

Derecho a la confidencialidad de la información estipulado en la constitución política del Ecuador

 **16:10 ¶ 20 in Case 16**

La respuesta es no, porque si yo estoy proporcionando mi información, es porque se donde la voy a colocar. En caso de que la empresa en donde proporcioné mis datos los haga públicos para que sean vulnerados, tomaría acciones legales. Si yo publico algo personal, al hacerlo público, estoy asumiendo el riesgo. Recalco, si la empresa infringe, el derecho que se viola es el de la privacidad y dependiendo de que pase con los datos, se generaría una cadena de violación de derechos de diferentes tipos.

 **17:10 ¶ 20 in Case 17**

Todo dato que se proporcione esta sujeto a violentarse. (Corrupción)

 **18:10 ¶ 20 in Case 18**


Si, a la violación de la privacidad e integridad de la información sin previa autorización

 **19:10 ¶ 20 in Case 19**

Definitivamente, por eso lo expresado en puntos anteriores en el sentido de que la información recopilada debe contar con todas las seguridades del caso

 **20:10 ¶ 20 in Case 20**


Si mis datos personales son empleados de mala manera si se violan los derechos de privacidad

 **7. ¿Cree que la práctica de recolección de datos mediante cookies o métodos de captación de información adicional es indiscriminada, al recopilar datos sin conocimiento ni consentimiento del usuario? Qué puede provocar? (Desarrolle su respuesta)**

20 Citas:

 **1:11 ¶ 22 in Case 1**

Los mecanismos tecnológicos pueden servir para robo de información que atente contra el derecho a la intimidad

 **2:11 ¶ 22 in Case 2**

Si, debe ser una autorización expresa

 **3:11 ¶ 22 in Case 3**

Puede ser porque en todo caso se obtiene información sin consentimiento

 **4:11 ¶ 22 in Case 4**


Si es indiscriminada porque es ahí cuando el usuario o el consumidor se ve limitado de rechazarlas o aceptarlas, en caso de no estar de acuerdo de aceptar no puedo usarla.

 **5:11 ¶ 22 in Case 5**


Si es una violación de derecho a la privacidad

 **6:11 ¶ 22 in Case 6**

Por lo general yo he observado páginas que advierten al usuario que están utilizando cookies. Éste es un modo de prevención implantado en internet, justamente para evitar que se recolecten datos sin aprobación del usuario

 **7:11 ¶ 22 in Case 7**

Provoca invasión de espacios privados como el descanso, o el mismo trabajo. Gracias a sus algoritmos de focalización de tendencias consumistas, contactan por varios medios a los usuarios para ofrecerles bienes o servicios no requeridos, es decir ejercen presión para que el usuario adquiera obligaciones con consentimiento inducido.

 **8:11 ¶ 22 in Case 8**

Lo es, y eso se debe a la falta de control de la obtención de información y la adecuación legal a esta gran industria del internet, aún hay muchos modos/ delitos que no constan en la legislación y deben ser considerados para limitar dicho acceso ilegal

 **9:11 ¶ 22 in Case 9**

Si es indiscriminada pero también los usuarios son imprudentes y lo permiten para acceder a determinadas páginas. Lo que puede provocar es lo que hemos anotado, violación de nuestra vida privada

 **10:11 ¶ 22 in Case 10**

Puede provocar que te llenan de notificaciones de todas las empresa que compraron esa data para su marketing, provocar que te asalten en la entrada de tu casa porque publicaste tu dirección completa, estas expuesto a infinidad de situaciones

 **11:11 ¶ 22 in Case 11**

Si el usuario está de acuerdo al ingresar a la plataforma debe estar consiente que su información se hará pública

 **12:11 ¶ 22 in Case 12**

Ellos manejan buenas estrategias de marketing muy persuasivas y manipuladoras que sutilmente obtienen nuestros datos, supuestamente ellos nos piden nuestro consentimiento, pero esto es algo estratégico q a veces no nos damos cuenta que lo hacemos

 **13:11 ¶ 22 in Case 13**

Generaría desconfianza al uso de las tecnologías

 **14:11 ¶ 22 in Case 14**

Existen datos que pueden facilitar a terceros para causar daño a cualquier persona dañando su buen nombre

 **15:11 ¶ 22 in Case 15**


Puede provocar filtración de información confidencial como claves y contraseñas

 **16:11 ¶ 22 in Case 16**


En el caso de que eso se produzca, lo cual es muy raro, ya que toda aplicación desarrollada por una empresa que sea formal, siempre notificará que el guardado de las cookies o data se hará. Si en caso, la empresa no notifica mediante mensajes de aplicación, es muy seguro de que no sea una empresa legal y obtenga esta información con la finalidad de delinquir.

 **17:11 ¶ 22 in Case 17**


Si puede provocar que muchas personas alteren sus malos pensamientos y se desarrolle ganancias deshonestas.

 **18:11 ¶ 22 in Case 18**

No necesariamente ya que las cookies guardan solo cierta información para hacer que la navegación web sea mas sencilla y el usuario indica en un pop up de alerta si desea autorizar las cookies para el sitio de navegación

 **19:11 ¶ 22 in Case 19**

Si porque no se asegura de que el usuario este consciente que permite al consentir la utilización de cookies, esto puede provocar abusos de terceros escudados en el consentimiento del usuario

 **20:11 ¶ 22 in Case 20**

La recolección de datos mediante cookies afecta la privacidad y puede exponer a los usuarios.

◇ ○ 8. Para el usuario, ¿Qué consecuencias traería la recolección de sus datos por parte de empresas y entidades gubernamentales? Conoce el proceso? (Desarrolle su respuesta)

20 Citas:

☰ 1:12 ¶ 24 in Case 1

La pérdida del anonimato

☰ 2:12 ¶ 24 in Case 2

El abuso de información personal

☰ 3:12 ¶ 24 in Case 3

En negativa porque no tiene ni goza mi consentimiento, ya que si me siento vulnerada activaría los mecanismos legales

☰ 4:12 ¶ 24 in Case 4

Ellos captan datos de distinta fuentes, usurpando información porqué dan inicio a una actividad en dónde la recolección de información obedece a implementar otros procedimientos para recopilar información focalizada. Y si no cuentan exclusivamente con la autorización para aquello estaría vulnerando mi derecho a la intimidad personal.

☰ 5:12 ¶ 24 in Case 5

Puede ser producto de un hakeo y que pueda dar mal uso


☰ 6:12 ¶ 24 in Case 6

La consecuencia negativa depende de algo que no va a estar escrito en un libro o ninguna normativa, y eso es la intención, por ejemplo estaríamos hablando de que puede ser beneficioso si el estado utiliza esos datos, para capturar delincuentes, pero sería sumamente dañino si tales datos fueran usados para perseguir opositores del gobierno.


Obviamente es muy difícil separar lo uno del otro, por ejemplo para perseguir a un enemigo político podría alegarse que éste ha cometido un delito.

 **7:12 ¶ 24 in Case 7**


Implica el riesgo de exposición política, mediática, o ante organizaciones delincuenciales.

 **8:12 ¶ 24 in Case 8**


No conozco el proceso, sin embargo, ninguna información obtenida sin Consentimiento, debe ser usada por terceros con fines lucrativos, el derecho a la intimidad del ciudadano debe prevalecer, salvo claro, casos legales específicos

 **9:12 ¶ 24 in Case 9**


No sé el proceso en si. No deberían desviarse los fines de la recolección de datos.

 **10:12 ¶ 24 in Case 10**

la recolección de datos toda empresa lo hace de acuerdo al giro de su negocio y esta bien, el problema es que seguridades tiene par esos datos y que hace con esa data de acuerdo a ellos los usuarios sufrimos las consecuencias

 **11:12 ¶ 24 in Case 11**

No conozco el proceso, pero la información del estado es pública por ello si la persona está consciente de ello, sabrá las consecuencias a futuro

 **12:12 ¶ 24 in Case 12**

Las consecuencias son muchas, entre ellas manipular y hacernos comprar cosas q no queremos o deseamos, en tema político puede hacernos votar por algún candidato q no queremos y así un sinnúmero de actos negativos

 **13:12 ¶ 24 in Case 13**

No lo conozco

 **14:12 ¶ 24 in Case 14**


La pérdida del anonimato

 **15:12 ¶ 24 in Case 15**


Como consecuencia principal está el riesgo de filtración de información

 **16:12 ¶ 24 in Case 16**

Todo usuario es un ciudadano, y todo ciudadano, debe rendir cuentas al país. Por ende, todos de una forma u otra, acceden a plataformas gubernamentales para realizar diferentes trámites. Mientras la data sea del tipo que es necesaria para el gobierno de turno, entonces, estaría correcto. Para algo diferente a esto, no debe de producirse.

 **17:12 ¶ 24 in Case 17**

Por ejemplo: El SRI, sabemos que debemos declarar facturas y no se lo hace como debe de ser. Por ende la entidad trae como consecuencia una multa. (la misma que puede ser desviada por corrupción)

 **18:12 ¶ 24 in Case 18**

Desconozco el proceso, sin embargo, a mi criterio las consecuencias podrían ser la exposición de información persona, datos, videos, fotos, audios a terceras personas sin la debida autorización del usuario

 **19:12 ¶ 24 in Case 19**

Puede ser objeto de persecución en un momento de su vida si el gobierno de turno así lo ordena.

 **20:12 ¶ 24 in Case 20**

La recolección de datos por parte de empresas o del Estado como los Censos ayuda a la planificación pero debe ser empleada de manera responsable.

◇ ○ 9. ¿Tiene conocimiento si la recolección de información de datos digitales está normada legalmente por el Estado Ecuatoriano? (Desarrolle su respuesta)

20 Citas:

☰ 1:13 ¶ 26 in Case 1

No, porque existe todo el acceso a internet no está regulado, existiendo una responsabilidad ulterior

☰ 2:13 ¶ 26 in Case 2

No, es deficiente, falta regulación normativa por parte de la Asamblea Nacional

☰ 3:13 ¶ 26 in Case 3

No, debería de ser normado y debería de existir una normativa bastante fuerte para ello

☰ 4:13 ¶ 26 in Case 4

No se encuentra mayormente legislado a nivel nacional

☰ 5:13 ¶ 26 in Case 5


No, tiene que ser más específica y protectora

☰ 6:13 ¶ 26 in Case 6


Esta norma hasta cierto punto, pero no es una normativa completa y suficiente, lo poco que está normado no se lo aplica eficientemente. Por ejemplo, resulta tarea imposible tratar de quejarme por las distintas llamadas a mi teléfono ofreciéndome productos.

☰ 7:13 ¶ 26 in Case 7


Lo está de manera dispersa. Se supone que todas las entidades públicas, por ejemplo, pueden recolectar la información y solo pueden usarla para los fines institucionales. Las privadas se fundamentan en el consentimiento forzado que el usuario brinda en los contratos de adhesión.

 **8:13 ¶ 26 in Case 8**


No tengo información concreta, pero sé que si hay delitos establecidos, relacionados, en el COIP con actos de uso indebidos o alteraciones de sistemas y datos. Es posible que con la teoría del caso adecuado, se ajuste a esos delitos Normandos en la legislación penal ecuatoriana

 **9:13 ¶ 26 in Case 9**


Se ha legislado algo

 **10:13 ¶ 26 in Case 10**


No lo sé hasta donde este normado

 **11:13 ¶ 26 in Case 11**


Así es la información y el acceso a ella tiene normas

 **12:13 ¶ 26 in Case 12**


No tengo pleno conocimiento de eso, pero creo que el estado Ecuatoriano no tiene normando este tema

 **13:13 ¶ 26 in Case 13**

No tengo conocimiento

 **14:13 ¶ 26 in Case 14**

Es deficiente deberían de ser reguladas...

 **15:13 ¶ 26 in Case 15**

Si

 **16:13 ¶ 26 in Case 16**


Si tengo conocimiento, pero no cubre la totalidad de lo que se necesita.

 **17:13 ¶ 26 in Case 17**

Debe estar normado, pero como la tecnología ha avanzado el estado debería a estas alturas ya normalizar. Por ejemplo: compras en el exterior, retención de IVA, impuestos.

 **18:13 ¶ 26 in Case 18**

No tenía conocimiento al respecto

 **19:13 ¶ 26 in Case 19**


Entiendo que si pero no conozco detalles

 **20:13 ¶ 26 in Case 20**

Desconozco

 **○ Actividad de su profesión**

20 Citas:

 **1:4 ¶ 8 in Case 1**

Juez de la Sala Civil de la Corte Provincial del Guayas

 **2:4 ¶ 8 in Case 2**

Juez de la Sala Laboral de la Corte Provincial del Guayas

 **3:4 ¶ 8 in Case 3**

Jueza de la Civil de la Corte Provincial del Guayas

 **4:4 ¶ 8 in Case 4**

Juez de la Sala Especializada de lo Civil de la Corte Provincial del Guayas

 **5:4 ¶ 8 in Case 5**

Juez de la Sala Especializada de lo Civil de la Corte Provincial del Guayas

 **6:4 ¶ 8 in Case 6**


Juez de la Sala Especializada de lo Civil de la Corte Provincial del Guayas

 **7:4 ¶ 8 in Case 7**

Juez

 **8:4 ¶ 8 in Case 8**

Judicial

 **9:4 ¶ 8 in Case 9**


Juez

 **10:4 ¶ 8 in Case 10**


Ingeniera en sistemas

 **11:4 ¶ 8 in Case 11**

Analista de Articulación

 **12:4 ¶ 8 in Case 12**

Ingeniero en Marketing y negociación comercial

 **13:4 ¶ 8 in Case 13**

Combustibles

 **14:4 ¶ 8 in Case 14**

Abogada

 **15:4 ¶ 8 in Case 15**


Docente

 **16:4 ¶ 8 in Case 16**

Ingeniero TI

 **17:4 ¶ 8 in Case 17**


Sistemas, Telecomunicación e Industrial

 **18:4 ¶ 8 in Case 18**

Ingeniero en sistemas

 **19:4 ¶ 8 in Case 19**


Consultor de Sistemas SAP

 **20:4 ¶ 8 in Case 20**

Técnico

 ○ **En base al derecho contemplado en el numeral 2 del Art. 16 de la Constitución del Ecuador que determina**

1 Citas:

 **1:18 ¶ 9 – 32 in Case 1**

En base al derecho contemplado en el numeral 2 del Art. 16 de la Constitución del Ecuador que determina: "Todas las personas, en forma individual o colectiva, tienen derecho a: El acceso universal a las tecnologías de información y comunicación". Cree

usted que su ejercicio tendría como efecto la vulneración de otros derechos de los ciudadanos, contemplados en la Constitución y Tratados Internacionales de Derechos Humanos? ¿Cuáles? y ¿Por qué? (Desarrolle su respuesta)

No, por qué no se visualiza la violación de derechos con el acceso a las TIC, más ayuda a desarrollar tareas en el ámbito educativo y laboral

2. ¿Cómo cree usted que las Tecnologías de la Información y Comunicación (TICs), Redes Sociales y aplicaciones tecnológicas, causan o causarían violación de derechos a los usuarios?Cuál sería el proceso para esto? (Desarrolle su respuesta)

Para acceder a un programa solicitan una autorización y por lo tanto se debe sujetarse a un contrato de adhesión para su utilización, por lo que está en el usuario el derecho de acceder o no a las mismas

3. ¿Qué opinión le merece, el uso que las empresas desarrolladoras de tecnología y el Estado dan a los datos o información obtenida de los usuarios, mediante cualquier plataforma tecnológica? (Desarrolle su respuesta)

La captación de información de los usuarios expone al ciudadano a que sus datos puedan ser utilizados por corporaciones o estados para un control social o venta de información respecto de los gustos de los clientes o usuarios.

4. Cómo experto, que situaciones pueden realizarse con la información o datos recopilados por el sistema de cámaras de seguridad instalada en áreas públicas por el Estado? Esto, podría afectar de alguna manera a los derechos de los ciudadanos? (Desarrolle su respuesta)

El desarrollo tecnológico a llevado a que la humanidad tenga que pagar un precio por el mismo lo que conlleva a que los ciudadanos pierdan parte de su privacidad a través de la recuperación de información

5. Cuál es su opinión sobre el uso que se podría dar a los datos que recolectan las Empresas y el Estado. Tiene alguna consecuencia negativa en relación a los derechos de los ciudadanos? (Desarrolle su respuesta)

Repercute directamente en el derecho a la intimidad y a una posible utilización de dicha información para fines que atenten contra la dignidad de las personas o su integridad física inclusive la vida

6. Cómo usuario de internet y redes sociales, cree que la información o datos personales proporcionada por usted, serviría para se configure la violación de sus derechos? Cuáles derechos sería y por qué? (Desarrolle su respuesta)

Si, porqué a través de estos algoritmos que manejan estas súper computadoras permiten establecer patrones de conducta, frecuencias en cuanto a gusto de las personas

7. ¿Cree que la práctica de recolección de datos mediante cookies o métodos de captación de información adicional es indiscriminada, al recopilar datos sin conocimiento ni consentimiento del usuario? Qué puede provocar? (Desarrolle su respuesta)

Los mecanismos tecnológicos pueden servir para robo de información que atente contra el derecho a la intimidad

8. Para el usuario, ¿Qué consecuencias traería la recolección de sus datos por parte de empresas y entidades gubernamentales? Conoce el proceso? (Desarrolle su respuesta)

La pérdida del anonimato

9. ¿Tiene conocimiento si la recolección de información de datos digitales está normado legalmente por el Estado Ecuatoriano? (Desarrolle su respuesta)

No, porqué existe todo el acceso a internet no está regulado, existiendo una responsabilidad ulterior

10. ¿Cree usted que el Estado Ecuatoriano debería de normar el uso, captación y venta de datos de usuarios por parte de la Empresas desarrolladoras tecnológicas y de las entidades gubernamentales? (Desarrolle su respuesta)

Si, la información de los ciudadanos no podría estar en manos de personas particulares que hagan uso comercial de las mismas

11. ¿Considera que el desarrollo de las TICs, software y programas como la inteligencia artificial podrían vulnerar derechos? Cuáles y por qué? (Desarrolle su respuesta)


Generan vulneración de derechos, como el derecho a la intimidad, honra y buen nombre

12. En su opinión, ¿Cuál sería, la forma óptima y segura de utilizar las TIC, Redes Sociales y Aplicaciones tecnológicas? para evitar la captación de nuestra información y no ser víctimas de vulneración de derechos? (Desarrolle su respuesta)


Es necesario eliminar mecanismos que no permitan rastrear al ciudadanos

 **○ Marca temporal**


20 Citas:

 **1:1 ¶ 2 in Case 1**


08/13/2021 15:46:39

 **2:1 ¶ 2 in Case 2**


08/13/2021 16:14:43

 **3:1 ¶ 2 in Case 3**


08/13/2021 16:31:48


 **4:1 ¶ 2 in Case 4**


08/13/2021 17:19:44


 **5:1 ¶ 2 in Case 5**


08/13/2021 17:52:30


 **6:1 ¶ 2 in Case 6**
08/13/2021 18:40:11


 **7:1 ¶ 2 in Case 7**
08/13/2021 22:12:49


 **8:1 ¶ 2 in Case 8**
08/14/2021 20:24:03


 **9:1 ¶ 2 in Case 9**
08/14/2021 23:31:52


 **10:1 ¶ 2 in Case 10**
08/15/2021 04:24:39

 **11:1 ¶ 2 in Case 11**
08/15/2021 11:24:37

 **12:1 ¶ 2 in Case 12**
08/15/2021 19:46:04


 **13:1 ¶ 2 in Case 13**
08/15/2021 20:05:56

 **14:1 ¶ 2 in Case 14**
08/15/2021 20:19:37

 **15:1 ¶ 2 in Case 15**
08/15/2021 20:26:47

 **16:1 ¶ 2 in Case 16**


08/15/2021 20:33:28

 **17:1 ¶ 2 in Case 17**

08/15/2021 21:07:08

 **18:1 ¶ 2 in Case 18**

08/15/2021 22:31:30

 **19:1 ¶ 2 in Case 19**


08/16/2021 00:28:05

 **20:1 ¶ 2 in Case 20**


08/16/2021 07:12:09

 **○ Nombre y Apellidos del entrevistado**

20 Citas:

 **1:2 ¶ 4 in Case 1**


Amado Joselito Romero Galarza

 **2:2 ¶ 4 in Case 2**

Marco Jirón Coronel

 **3:2 ¶ 4 in Case 3**

María Gabriela Mayorga Contreras

 **4:2 ¶ 4 in Case 4**

Manuel Ulises Torres Soto

 **5:2 ¶ 4 in Case 5**


Gil Medardo Armijos Borja

 **6:2 ¶ 4 in Case 6**

José Villagran Cepeda

 **7:2 ¶ 4 in Case 7**

Dorian Rodriguez Silva

 **8:2 ¶ 4 in Case 8**

Laura Sabando

 **9:2 ¶ 4 in Case 9**

Shirley Ronquillo Bermeo

 **10:2 ¶ 4 in Case 10**

elsa alarcon

 **11:2 ¶ 4 in Case 11**


Cristhian García Guaman

 **12:2 ¶ 4 in Case 12**


Mario Moncayo zumba


 **13:2 ¶ 4 in Case 13**


Jonathan Diaz Mendoza


 **14:2 ¶ 4 in Case 14**


Katherine Bejar


 **15:2 ¶ 4 in Case 15**
Quinto Ochoa Edmundo

 **16:2 ¶ 4 in Case 16**
Santiago jimenez garcia

 **17:2 ¶ 4 in Case 17**
Jose Luis Farias Betty


 **18:2 ¶ 4 in Case 18**
Anthony Xavier Solis Mora


 **19:2 ¶ 4 in Case 19**
Alfredo Gutiérrez López


 **20:2 ¶ 4 in Case 20**
Gustavo Pilamunga Llumiguano

 ○ **Título Universitario**


20 Citas:

 **1:3 ¶ 6 in Case 1**
Abogado


 **2:3 ¶ 6 in Case 2**
Abogado

 **3:3 ¶ 6 in Case 3**


Abogado

 **4:3 ¶ 6 in Case 4**

Abogado

 **5:3 ¶ 6 in Case 5**

Abogado

 **6:3 ¶ 6 in Case 6**


Abogado

 **7:3 ¶ 6 in Case 7**

Abogado

 **8:3 ¶ 6 in Case 8**

Abogado

 **9:3 ¶ 6 in Case 9**


Abogado

 **10:3 ¶ 6 in Case 10**


Ingeniero en Sistemas, TIC o afines

 **11:3 ¶ 6 in Case 11**


Ingeniero en Sistemas, TIC o afines

 **12:3 ¶ 6 in Case 12**


Ingeniero en Sistemas, TIC o afines

 **13:3 ¶ 6 in Case 13**


Ingeniero en Sistemas, TIC o afines

 **14:3 ¶ 6 in Case 14**

Abogado

 **15:3 ¶ 6 in Case 15**


Ingeniero en Sistemas, TIC o afines

 **16:3 ¶ 6 in Case 16**

Ingeniero en Sistemas, TIC o afines

 **17:3 ¶ 6 in Case 17**


Ingeniero en Sistemas, TIC o afines

 **18:3 ¶ 6 in Case 18**

Ingeniero en Sistemas, TIC o afines

 **19:3 ¶ 6 in Case 19**


Ingeniero en Sistemas, TIC o afines

 **20:3 ¶ 6 in Case 20**

Ingeniero en Sistemas, TIC o afines

 ○ **"Todas las personas, en forma individual o colectiva, tienen derecho a**

1 Citas:

 **1:18 ¶ 9 – 32 in Case 1**

En base al derecho contemplado en el numeral 2 del Art. 16 de la Constitución del Ecuador que determina: "Todas las personas, en forma individual o colectiva, tienen derecho a: El acceso universal a las tecnologías de información y comunicación". ¿Cree usted que su ejercicio tendría como efecto la vulneración de otros derechos de los

ciudadanos, contemplados en la Constitución y Tratados Internacionales de Derechos Humanos? ¿Cuáles? y ¿Por qué? (Desarrolle su respuesta)

No, por qué no se visualiza la violación de derechos con el acceso a las TIC, más ayuda a desarrollar tareas en el ámbito educativo y laboral

2. ¿Cómo cree usted que las Tecnologías de la Información y Comunicación (TICs), Redes Sociales y aplicaciones tecnológicas, ¿causan o causarían violación de derechos a los usuarios? ¿Cuál sería el proceso para esto? (Desarrolle su respuesta)

Para acceder a un programa solicitan una autorización y por lo tanto se debe sujetarse a un contrato de adhesión para su utilización, por lo que está en el usuario el derecho de acceder o no a las mismas

3. ¿Qué opinión le merece, el uso que las empresas desarrolladoras de tecnología y el Estado dan a los datos o información obtenida de los usuarios, mediante cualquier plataforma tecnológica? (Desarrolle su respuesta)

La captación de información de los usuarios expone al ciudadano a que sus datos puedan ser utilizados por corporaciones o estados para un control social o venta de información respecto de los gustos de los clientes o usuarios.

4. Cómo experto, que situaciones pueden realizarse con la información o datos recopilados por el sistema de cámaras de seguridad instalada en áreas públicas por el Estado? ¿Esto, podría afectar de alguna manera a los derechos de los ciudadanos? (Desarrolle su respuesta)

El desarrollo tecnológico a llevado a que la humanidad tenga que pagar un precio por el mismo lo que conlleva a que los ciudadanos pierdan parte de su privacidad a través de la recuperación de información

5. Cuál es su opinión sobre el uso que se podría dar a los datos que recolectan las Empresas y el Estado. ¿Tiene alguna consecuencia negativa en relación a los derechos de los ciudadanos? (Desarrolle su respuesta)

Repercute directamente en el derecho a la intimidad y a una posible utilización de dicha información para fines que atenten contra la dignidad de las personas o su integridad física inclusive la vida

6. Cómo usuario de internet y redes sociales, cree que la información o datos personales proporcionada por usted, ¿serviría para se configure la violación de sus derechos? ¿Cuáles derechos sería y por qué? (Desarrolle su respuesta)

Si, porqué a través de estos algoritmos que manejan estas súper computadoras permiten establecer patrones de conducta, frecuencias en cuanto a gusto de las personas

7. ¿Cree que la práctica de recolección de datos mediante cookies o métodos de captación de información adicional es indiscriminada, al recopilar datos sin conocimiento ni consentimiento del usuario? ¿Qué puede provocar? (Desarrolle su respuesta)

Los mecanismos tecnológicos pueden servir para robo de información que atente contra el derecho a la intimidad

8. Para el usuario, ¿Qué consecuencias traería la recolección de sus datos por parte de empresas y entidades gubernamentales? ¿Conoce el proceso? (Desarrolle su respuesta)

La pérdida del anonimato

9. ¿Tiene conocimiento si la recolección de información de datos digitales está normada legalmente por el Estado Ecuatoriano? (Desarrolle su respuesta)

No, porqué existe todo el acceso a internet no está regulado, existiendo una responsabilidad ulterior

10. ¿Cree usted que el Estado Ecuatoriano debería de normar el uso, captación y venta de datos de usuarios por parte de la Empresas desarrolladoras tecnológicas y de las entidades gubernamentales? (Desarrolle su respuesta)

Si, la información de los ciudadanos no podría estar en manos de personas particulares que hagan uso comercial de las mismas

11. ¿Considera que el desarrollo de las TICs, software y programas como la inteligencia artificial podrían vulnerar derechos? ¿Cuáles y por qué? (Desarrolle su respuesta)

Generan vulneración de derechos, como el derecho a la intimidad, honra y buen nombre

12. En su opinión, ¿Cuál sería, la forma óptima y segura de utilizar las TIC, Redes Sociales y Aplicaciones tecnológicas? para evitar la captación de nuestra información y no ser víctimas de vulneración de derechos? (Desarrolle su respuesta)

Es necesario eliminar mecanismos que no permitan rastrear al ciudadano.

DECLARACIÓN Y AUTORIZACIÓN

Yo, Omar Gerard Altamirano, con C.C: # 120580735-5 autor del trabajo de titulación: **El acceso a las Tecnologías de la Información y Comunicación (TICS) como derecho establecido en la constitución del Ecuador de 2008 y su efecto sistemático de vulneración de derechos de los ciudadanos.** Previo a la obtención del título de **Magister en Derecho Constitucional** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 11 noviembre del 2021.

f. _____

Abg. Omar Gerard Altamirano
C.C: 120580735-5

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE GRADUACIÓN

TÍTULO Y SUBTÍTULO:	El acceso a las Tecnologías de la Información y Comunicación (TICS) como derecho establecido en la constitución del Ecuador de 2008 y su efecto sistemático de vulneración de derechos de los ciudadanos.		
AUTOR(ES) (apellidos/nombres):	Abg. Omar Gerard Altamirano Villena		
REVISOR(ES)/TUTOR(ES) (apellidos/nombres):	Abg. Kleber David Sigüencia Suarez, Mgtr; Dra. Nuria Pérez Puig-Mir; Lcda. María Verónica Peña Seminario, Phd.		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
UNIDAD/FACULTAD:	Sistema de Posgrado		
MAESTRÍA/ESPECIALIDAD:	Maestría en Derecho Constitucional		
GRADO OBTENIDO:	Magíster en Derecho Constitucional		
FECHA DE PUBLICACIÓN:	11 de noviembre del 2021	No. DE PÁGINAS:	210
ÁREAS TEMÁTICAS:	Derecho Constitucional		
PALABRAS CLAVES/ KEYWORDS:	Vulneración de Derechos, Derecho a la privacidad, Internet, Ciudadanos, Gobierno, Empresas tecnológicas, TIC, Tecnología, Redes Sociales, aplicaciones, cámaras de vigilancia, Datos, Tratamiento de Datos personales.		
RESUMEN/ABSTRACT (150-250 palabras):	<p>A partir de que la Organización de las Naciones Unidas (ONU) declaró el acceso a internet como un derecho humano, instando a los gobiernos a facilitar su acceso, mencionando que es una herramienta que facilita el crecimiento y progreso de las sociedades, además de la utilidad para ejercer el derecho a la libertad de expresión, muchos países incluyendo a Ecuador han creado profundas reformas en sus leyes para lograr este objetivo, es así que la Constitución de la República del Ecuador del 2008, establece el derecho al acceso de las Tecnologías de la Información y Comunicación de los ciudadanos ecuatorianos, con el fin de integrar a los ciudadanos a la sociedad de la información y del conocimiento, asegurando el acceso y uso del internet.</p> <p>Sin embargo, en la práctica existen perjuicios que atentan tanto al ciudadano individual, como a la sociedad. Al ejercer el derecho al acceso de las TICs, la falta de conocimiento y capacitación de su debida aplicación, sumada la irresponsabilidad del ciudadano, además de una deficiente legislación en la materia, se generan violaciones a los derechos de los ciudadanos; violaciones realizadas no sólo por las empresas tecnológicas con su recolección y tratamiento de datos, sino también por los gobiernos de los Estados al ejercer políticas públicas de control.</p> <p>En la actualidad, la irrupción de la tecnología es abrumadora, su desarrollo acelerado, es una debilidad del derecho que evoluciona de forma lenta y paulatina, por lo cual, valiéndose de la democratización del acceso a las TICs, en la cual los usuarios crecen, los datos han reemplazado al petróleo, siendo su utilización y aplicación para fines comerciales y políticos no ha conocido limites, causando perjuicios y por ende violaciones de derechos, los cuales se han expuesto en el presente estudio. <input type="checkbox"/></p>		
ADJUNTO PDF:	<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO	
CONTACTO CON AUTORES/ES:	Teléfono: 0992176342	E-mail: omar.altamirano.villena@hotmail.com	
CONTACTO CON LA INSTITUCIÓN:	Nombre: Hernández Terán Miguel Antonio		
	Teléfono: 0985219697		
	E-mail: mhtjuridico@gmail.com		
SECCIÓN PARA USO DE BIBLIOTECA			
Nº. DE REGISTRO (en base a datos):			
Nº. DE CLASIFICACIÓN:			
DIRECCIÓN URL (tesis en la web):			